INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

October 4, 2019
Ref: FOIA-2016-00048

SENT VIA EMAIL TO: 21270-23321484@requests.muckrock.com
Mr. Patrick H. O'Neill
MuckRock
DEPT MR 21270
P.O. Box 55819
Boston, MA 02205-5819

Dear Mr. O'Neill:

This responds to your Freedom of Information Act (FOIA) request for a copy of report DODIG-2015-168, (U) Air Force Commands Need to Improve Logical and Physical Security Safeguards that Protect SIPRNet Access Points. We received your request on October 15, 2015, and assigned it case number FOIA-2016-00048.

The Office of the Deputy Inspector General for Audit conducted a search and found the enclosed record responsive to your request. In coordination with the Department of the Air Force, we determined that redacted portions are exempt from release pursuant to the following FOIA exemptions:

- 5 U.S.C. § 552 (b)(1), which pertains to information that is currently and properly classified pursuant to Executive Order 13526, Section 1.4(g), as it relates to vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security;

- 5 U.S.C. § 552 (b)(3), which pertains to information exempted from release by statute, in this instance 10 U.S.C. § 130e - Department of Defense critical infrastructure security information (DCRIT). Specifically, portions redacted under this statute contain sensitive but unclassified information related to the Department of Defense Information Network, which has been deemed to qualify as DCRIT by the Chief Management Officer of the Department of Defense;

- 5 U.S.C. § 552 (b)(5), which pertains to certain inter-and intra-agency communications protected by the deliberative process privilege;

- 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy; and

- 5 U.S.C. § 552 (b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

October 4, 2019
Ref: FOIA-2016-00048

If you consider this an adverse determination, you may submit an appeal. Your appeal, if any, must be postmarked within 90 days of the date of this letter, clearly identify the determination that you would like to appeal, and reference to the FOIA case number above. Send your appeal to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500, or via facsimile to 571-372-7498. For more information on appellate matters and administrative appeal procedures, please refer to 32 C.F.R. Sec. 286.9(e) and 286.11(a).

You may contact our FOIA Public Liaison at FOIAPublicLiaison@dodig.mil or by calling 703-604-9785, for any further assistance with your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records).

If you have any questions regarding this matter, please contact this office at 703-604-9775 or via email to foiarequests@dodig.mil.

Sincerely,

Searle Slutzkin
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

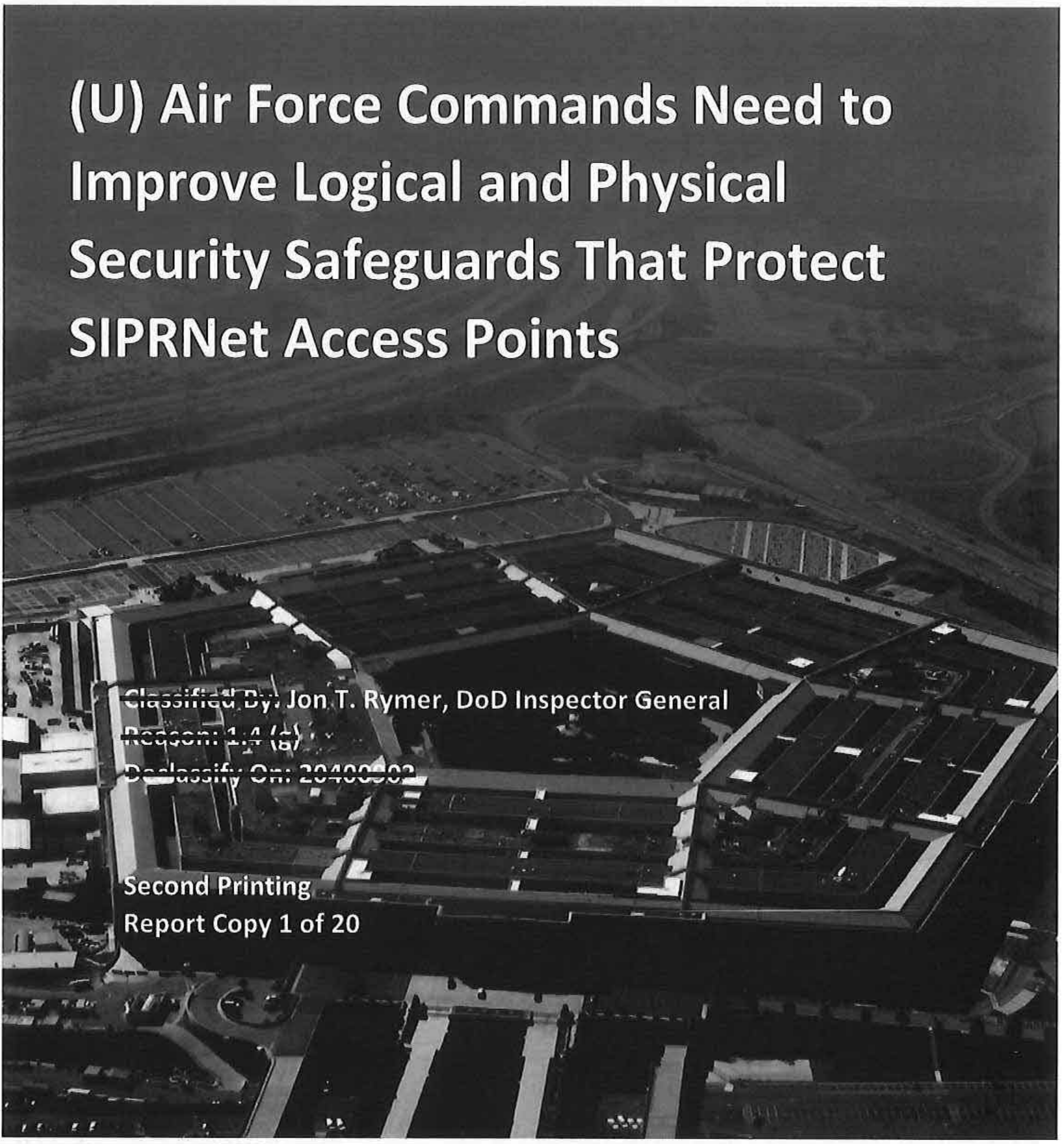
Project No. DODIG-2015-168

~~SECRET~~

INSPECTOR GENERAL

U.S. Department of Defense

September 3, 2015



(U) Air Force Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

~~Classified By:~~ Jon T. Rymer, DoD Inspector General
~~Reason: 1.4 (g)~~
~~Declassify On: 20400903~~

Second Printing
Report Copy 1 of 20

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~SECRET~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline|800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

(U) Air Force Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

September 3, 2015

(U) Objective

(U) Our audit objective was to determine whether the Air Force was effectively protecting its Secret Internet Protocol Router Network (SIPRNet) access points. Specifically, we reviewed the security safeguards that protect SIPRNet access points a (b) (7)(E) [redacted]

(U) Findings

~~(S)~~ Air Force commands (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. Specifically, among other findings, we found that (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] This occurred because (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] This occurred because (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

Security safeguards at (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] This occurred because DoD guidance (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. As a result, safeguards for the Air Force SIPRNet (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(U) Findings (cont'd)

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] in accordance with applicable DoD and Air Force guidance. This occurred because (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. As a result, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted].

(U) Management Actions Taken

~~(S)~~ During the audit, (b) (1), 1.4(g); (b) (7)(E) [redacted] In addition, (b) (1), 1.4(g); (b) (7)(E) [redacted].

Based on management actions taken, we do not have recommendations for these specific actions.

(U) Recommendations

~~(S)~~ Among other recommendations, we recommend that the Under Secretary of Defense for Intelligence, the Commander, U.S. Cyber Command, and the DoD Chief Information Officer (CIO) (b) (1), 1.4(g), (b) (7)(E) [redacted]; the Commander, Air Force Materiel Command, and the Commander, Air Force Reserve Command, (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]; the Chief, Information Dominance CIO review the deficiencies identified, require a thorough review of the Air Force SIPRNet security safeguards at each command and apply corrective actions as necessary; the Commander, (b) (7)(E) [redacted] and Commander, (b) (7)(E) [redacted], develop procedures to (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]; and the Commander, (b) (7)(E) [redacted], develop procedures to (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted].

~~(FOUO)~~ The Commander, (b) (7)(E) [redacted], should develop and implement a plan to (b) (3), 10 USC § 130e; (b) (7)(E) [redacted].

Results in Brief

(U) Air Force Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

(U) Management Comments and Our Response

(U) The Commander, U.S. Cyber Command; Director, Defense Information Systems Agency; and Commander, (b) (7)(E) [redacted] addressed the specifics of the recommendations.

(U) Comments from the Air Force Chief, Information Dominance CIO; Commander, (b) (7)(E) [redacted]; and Commander, (b) (7)(E) [redacted] partially addressed the recommendations. We request they provide additional comments in response to the final report. In addition, we received the Administrative Assistant to the Secretary of (U) the Air Force and DoD CIO comments on the draft report too late to include them in the final report. Therefore, if the Administrative Assistant to the Secretary of the Air Force and DoD CIO do not submit additional comments, we will consider those comments as the management response to the final report.

(U) The Under Secretary of Defense for Intelligence; Commander, Air Force Materiel Command; Commander, Air Force Space Command; Commander, Air Force Reserve Command; Commander, 24th Air Force; and Commander, (b) (7)(E) [redacted] did not provide comments to the draft report. We request that they respond to the final report. Please see the Recommendations Table on the next page.

(U) Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Intelligence	A.1	
Administrative Assistant to the Secretary of the Air Force	B.1	
Commander, Air Force Materiel Command	A.2	
Commander, U.S. Cyber Command		A.1, A.3
Commander, Air Force Space Command	A.4	
Department of Defense Chief Information Officer	A.1	
Director, Defense Information Systems Agency		A.3
Commander, Air Force Reserve Command	A.2	
Air Force Chief, Information Dominance Chief Information Officer	A.5.a, A.5.b, B.2	
Commander, 24th Air Force	A.6	
Commander, (b) (7)(E) [redacted]		A.7, B.3
Commander, (b) (7)(E) [redacted]	A.8.a, A.8.b, B.4.d	A.8.c, B.4.a, B.4.b, B.4.c
Commander, (b) (7)(E) [redacted]	B.5	A.9.a, A.9.b, A.9.c
Commander, (b) (7)(E) [redacted]	A.6, A.10.a, A.10.b, A.10.c, A.10.d	

(U) Please provide Management Comments by October 5, 2015.

September 3, 2015

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. CYBER COMMAND
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Air Force Commands Need to Improve Logical and Physical Controls That Protect SIPRNet Access Points (Report No. DODIG-2015-168)

~~(S)~~ We are providing this final report for your review and comment. We considered management comments on a draft of this report when preparing the final report. The Air Force commands (b)(3), 10 USC § 130e, (b)(7)(E) (b)(1), 1.4(g), (b)(3), 10 USC § 130e, (b)(7)(E). In addition, the Air Force commands (b)(1), 1.4(g), (b)(3), 10 USC § 130e, (b)(7)(E) complete SIPRNet access forms; and provide North Atlantic Treaty Organization briefings. We conducted this audit in accordance with generally accepted government auditing standards.

~~(FOUO)~~ DoD Instruction 7650.03 requires that all recommendations be resolved promptly. The Commander, U.S. Cyber Command; Director, Defense Information Systems Agency; and Commander, (b)(7)(E) addressed the specifics of the recommendations. Comments from the Air Force Chief, Information Dominance Chief Information Officer partially addressed Recommendation A.5.a and did not address Recommendations A.5.b and B.2. Therefore, we request additional comments on these recommendations by October 5, 2015. Comments from the Commander, (b)(7)(E) did not address Recommendations A.8.a, A.8.b, and B.4.d. Therefore, we request additional comments on these recommendations by October 5, 2015. Comments from the Commander, (b)(7)(E) did not address Recommendation B.5. Therefore, we request additional comments on these recommendations by October 5, 2015. We received the Administrative Assistant to the Secretary of the Air Force and DoD Chief Information Officer comments on the draft report too late to include them in the final report. Therefore, if the Administrative Assistant to the Secretary of the Air Force and DoD Chief Information Officer do not submit additional comments, we will consider those comments as the management response to the final report.

~~(FOUO)~~ The Under Secretary of Defense for Intelligence; Commander, Air Force Materiel Command; Commander, Air Force Space Command; Commander, Air Force Reserve Command; Commander, 24th Air Force; and Commander, (b)(7)(E) did not provide comments, and therefore, may not have taken any actions to correct or mitigate vulnerabilities identified in the report. The vulnerabilities identified were (b)(3), 10 USC § 130e, (b)(7)(E)

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]. It is required that these addressees respond to the recommendations in the final report with the actions taken to resolve these vulnerabilities by October 5, 2015.

(U) Please send a PDF file containing your comments to (b) (6) [redacted] and (b) (6) [redacted]. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified documents electronically, you must send them over the SIPRNet.

(U) We appreciate the courtesies extended to the staff. Please direct questions to (b) (6) [redacted] or (b) (6) [redacted]

Carol N. Gorman
Carol Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) Contents

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether the Air Force was effectively protecting its Secret Internet Protocol Router Network (SIPRNet) access points. Specifically, we reviewed the security safeguards that protected the SIPRNet access points at selected locations. This is the second in a series of audits to review the safeguards implemented by the Military Departments to protect SIPRNet access points. See Appendix A for our scope and methodology.

(U) Background

~~(FOUO)~~ SIPRNet access points are all possible physical or logical connections where a user can access SIPRNet. Physical safeguards such as locks, guards, and security containers deter or delay adversaries' access to the network. Logical safeguards are system-based mechanisms such as firewalls, permission settings, usernames and passwords, and SIPRNet tokens that are used to designate who or what has access to a specific system or function. Air Force Space Command manages the Air Force SIPRNet, and 24th Air Force operates the network.

~~(FOUO)~~ All Air Force bases connect to SIPRNet through (b)(7)(E) [redacted] access points called Gateways.[1] (b)(7)(E) [redacted] Gateways are located in the continental United States and (b)(7)(E) [redacted] are outside the continental United States. The Gateways control all network traffic in and out of the Air Force SIPRNet.[2] The data management responsibilities for SIPRNet are decentralized and divided among multiple squadrons that are subordinate to 24th Air Force and various Air Force major commands. (b)(7)(E) [redacted].[3] In addition, (b)(7)(E) [redacted]

[1] (U) Gateways are the entry and exit points for data to and from the SIPRNet.

[2] (U) The SIPRNet connects the Air Force classified enclaves to the Defense Information Systems Network.

[3] (U) Firewalls refer to hardware and software that limits access between networks or systems (or both) in accordance with a specific security policy.

[4] (U) Network defense devices include equipment used to monitor, detect, analyze, and respond and restore activities.

~~(FOUO)~~ The Gateways provide SIPRNet connection to the enclaves,[5] which support approximately 75,000 SIPRNet users. Figure 1 shows the flow of data between the access points, enclaves, and Gateways, and the squadrons that manage the SIPRNet.

(b)(7)(E) [redacted]

(U) Figure 1: Air Force SIPRNet Data Flow and Data Management Responsibilities

~~(FOUO)~~

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

~~(FOUO)~~

(U) [5] Enclaves are a collection of information systems connected by one or more internal networks under the control of a single authority and security policy.

(U) [6] The perimeter of a network encompasses all network components that are to be accredited by the designated accrediting authority.

(U) [7] Host Based Security System is an application that monitors, detects, and counters against known cyber threats.

(U) [8] The communications squadrons responsible for each base we reviewed were (b)(7)(E) [redacted] Communications Squadron at (b)(7)(E) [redacted], (b)(7)(E) [redacted] Communications Squadron at (b)(7)(E) [redacted], and (b)(7)(E) [redacted] Communications Squadron at (b)(7)(E) [redacted].

~~(FOUO)~~ We reviewed physical and logical safeguards for SIPRNet access points at the (b) (7)(E) [redacted] and three bases that are supported by the (b) (7)(E) [redacted]:

- (U) (b) (7)(E) [redacted];
- (U) (b) (7)(E) [redacted]; and
- (U) (b) (7)(E) [redacted].

(U) Vulnerability Categories

(U) DoD guidance[9] requires all vulnerabilities identified during Information Assurance (IA) control validation[10] be corrected or mitigated or that the risk be accepted. In addition, DoD Components[11] are required to report vulnerabilities on the Information Technology (IT) Security Plan of Action and Milestones (POA&M) before they grant an authorization to operate (ATO).[12] The IT Security POA&M assists agencies to identify, assess, prioritize, and monitor the DoD network's vulnerabilities and should include the actions performed to correct or mitigate the vulnerabilities. The IT Security POA&M should include the vulnerability and an assigned vulnerability severity category (CAT).

(U) CAT I vulnerabilities are assigned to findings that allow primary security protections to be bypassed, which allow immediate access by unauthorized personnel. Before an ATO is granted, all CAT I vulnerabilities are required to be corrected. For new CAT I vulnerabilities, the system can continue to operate on the network only if the designated accrediting authority certifies in writing that continued system operation is critical to mission accomplishment and the DoD Component Chief Information Officer (CIO) authorizes the system to continue to operate. Otherwise, the system must be disconnected from the SIPRNet.

(U) [9] DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007. The authorizations to operate for (b) (7)(E) [redacted] were issued under DoD Information Assurance Certification and Accreditation Process for up to three years and are applicable until recertification.

(U) [10] Validation confirms or establishes by testing, evaluation, examination, investigation, or competent evidence that a DoD information system assigned information assurance controls are implemented correctly.

(U) [11] DoD Components include Combatant Commands, Services, Agencies, and Field Activities.

(U) [12] Authorization to operate is an authorization granted by a designated accrediting authority for a DoD information system to process, store, or transmit information; an authorization to operate indicates a DoD information system has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the designated accrediting authority.

(U) Review of Internal Controls

(~~S~~) DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," May 30, 2013, requires DoD organizations to establish a program to review, assess, and report on the effectiveness of internal controls. We identified internal control weaknesses for 24th Air Force and (b)(7)(E). Specifically, (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E).[13] We will provide a copy of the report to the senior official responsible for internal controls at 24th Air Force and (b)(7)(E).

(~~S~~) We also identified internal control weaknesses for (b)(7)(E). Specifically, (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E). In addition, (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E); and validate that access forms and North Atlantic Treaty Organization (NATO) briefings were completed. We will provide a copy of the report to the senior official responsible for internal controls at (b)(7)(E).

(U) [13] A subnetwork is an identifiably separate part of an organization's network.

(U) [14] Port security refers to the electronic locking of network ports so that only approved devices can use the port.

(U) Finding A

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ The Air Force (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] Specifically:

- ~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

- ~~(FOUO)~~ (b) (7)(E) [redacted] Communications Squadron (CS), (b) (7)(E) [redacted], and (b) (7)(E) [redacted] CS, (b) (7)(E) [redacted], (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] This occurred because (b) (7)(E) [redacted] CS (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] and (b) (7)(E) [redacted] CS (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

- ~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. This occurred because (b) (7)(E) [redacted] CS and (b) (7)(E) [redacted] CS (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

- ~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(U) [15] Port security solutions are any method used to electronically lock network ports so that only approved devices can use the port.

(U) [16] Removable media are items such as compact discs, digital video disc, secure digital cards, tape, flash memory data storage devices, diskettes, multi-media cards, and external hard drives.

~~(FOUO)~~ [17] For this report, (b) (7)(E) [redacted]

- ~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]
- ~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]:

- ~~(FOUO)~~ (b) (7)(E) [redacted];
- ~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]
- ~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted].

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) [18] For this report, (b) (7)(E) [redacted].

(U) [19] Defense Information Systems Agency "Enclave" Security Technical Implementation Guide, Version 4, Release 4, January 9, 2014.

(U) [20] Deny-by-default is a configuration in which network traffic, which is not expressly allowed, is denied.

(U) [21] (b) (7)(E) [redacted]

(U) [22] (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

[redacted]

(U) [23] Boundary protection is monitoring and controlling communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications.

(U) [24] The authorizations to operate for (b) (7)(E) [redacted] were issued under DIACAP for up to three years and are applicable until recertification.

(U) [25] For the DIACAP, see Appendix B.

(U) [26] The Air Force Space Command submits Air Force ATOs to the Defense Information Systems Agency for approvals to connect to the Defense Information Systems Network.

~~(S)~~ (b)(1), 1.4(g), (b)(7)(E) [redacted]

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

~~(FOUO)~~ This occurred because (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]. After our site visit, (b)(7)(E) [redacted]. The Commander, Air Force Materiel Command and Commander, Air Force Reserve Command should review the bases under their command and implement a (b)(7)(E) [redacted] if needed.

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

~~(S)~~ (b)(1), 1.4(g), (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

(U) [27] Depending on where the Air Force ATOs are in the certification process will determine if the DIACAP or Risk Management Framework for DoD Information Technology applies. The Transition from the DIACAP to the Risk Management Framework for DoD Information Technology must not exceed the system re-authorization timeline.

(U) [28] Defense Information Systems Agency, "Access Control in Support of Information Systems," Security Technical Implementation Guide, Version 2, Release 3, October 29, 2010.

(U) [29] The Category I vulnerabilities were identified on the November 2014, December 2014, January 2015, February 2015, and March 2015 Assured Compliance Assessment Solution scans.

(U) [30] Assured Compliance Assessment Solution vulnerability scans.

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) Table. CAT I Vulnerability Scan Results

~~(S)~~

(b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) Note: The monthly scan results are located in Appendix C

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) [31] DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007.

(U) [32] Internet Protocol addresses are identifiers that are assigned to equipment connected to the network.

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) [33] (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) [34] The authorizations to operate for (b) (7)(E) [redacted] were issued under DIACAP for up to three years and are applicable until recertification.

(U) [35] (b) (7)(E) [redacted] CS reports to Air Combat Command and the (b) (7)(E) [redacted] CS reports to Air Force Materiel Command.

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

- ~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
- ~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
- ~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(U) [36] We used the control test table developed by DoD OIG Quantitative Methods Division and published in the Council of the Inspectors General on Integrity and Efficiency, "Journal of Public Inquiry," 2012-2013 when performing the control tests.

~~(FOUO)~~ [37] U.S. Cyber Command, Task Order 14-0185, "Insider Threat Mitigation," July 17, 2014 and Defense Information Systems Agency Program Executive Office – Mission Assurance Host Based Security System, "Device Control Module Guidance for Task Order 14-0185," October 28, 2014.

~~(S)~~ (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) [redacted]

~~(S)~~ (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) [redacted]

~~(S)~~ (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) [redacted]

(U) [38] The Office of the Secretary of Defense Memorandum "Insider Treat Mitigation," July 12, 2013, was signed by the Department of Defense, Chief Information Officer and the Under Secretary of Defense for Intelligence; however, U.S. Cyber Command is required to issue additional guidance.

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E)

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E)

~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E)

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E)

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E). We requested a list of users (b) (3), 10 USC § 130e; (b) (7)(E) during the 6-month period from August 2014 through January 2015 for each CS. (b) (3), 10 USC § 130e; (b) (7)(E), however, as a result of our audit, in May 2015, (b) (7)(E) CS identified approximately (b) (3), 10 USC § 130e; (b) (7)(E) We compared the lists provided by (b) (7)(E) to a list of current

~~(FOUO)~~ As a result of our audit, in May 2015, (b) (7)(E) identified approximately (b) (3), 10 USC § 130e; (b) (7)(E)

~~(FOUO)~~ users with SIPRNet access (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] In addition, while performing other tests of controls, we identified users (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. See Appendix D for our testing results.

~~(FOUO)~~ According to DoD[39] and Air Force[40] guidance, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ This occurred because (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] The Commander, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] according to DoD and Air Force guidance. If (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] cannot be developed then the Commander, (b) (7)(E) [redacted] should coordinate with base CSs and any other necessary parties to develop a (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] The Commander, (b) (7)(E) [redacted] in accordance with DoD and Air Force guidance.

(U) [39] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011.

(U) [40] Air Force Manual 33-282, "Computer Security," March 27, 2012; and Technical Manual Methods and Procedures, TO 00-33B-5004, "Access Control for Information Systems," December 19, 2012.

(U) [41] Active Directory provides a method to store data and provide data to network users and administrators.

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] SAF/CIO A6 should review the deficiencies identified, require a thorough review of the Air Force SIPRNet security safeguards performed at each command, and apply corrective actions as necessary.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation A.1

~~(FOUO)~~ We recommend that the Under Secretary of Defense for Intelligence, the Commander, U.S. Cyber Command, and the DoD Chief Information Officer, issue clarifying guidance for the Office of the Secretary of Defense Memorandum "Insider Threat Mitigation" to instruct Military Services and agencies on the proper procedures to (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) U.S. Cyber Command Comments

~~(FOUO)~~ The U.S. Cyber Command, Deputy Director, Current Operations, agreed, stating that the existing Defense Information Systems Agency Device Control Module guidance will be updated and released as of August 31, 2015. (b) (3), 10 USC § 130e, (b) (5), (b) (7)(E) [redacted] This will reinforce supporting documentation such as the

~~(FOUO)~~ February 11, 2014, White House memorandum "Near-Term Measures to Reduce the Risk of High Impact Unauthorized Disclosures" and the July 2, 2014, Office of the Secretary of Defense memorandum "Mitigations for Insider Threat and High Impact Unauthorized Disclosures."

(U) Our Response

(U) Comments from the Deputy Director addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

(U) DoD Chief Information Officer Comments

(U) We received the DoD CIO comments on the draft report too late to include them in the final report. Therefore, if the DoD CIO does not submit additional comments, we will consider those comments as the management response to the final report.

(U) Management Comments Required

(U) The Under Secretary of Defense for Intelligence did not provide comments to the draft report. Therefore, we request the Under Secretary provide comments in response to the final report.

(U) Recommendation A.2

~~(S)~~ We recommend that the Commander, Air Force Materiel Command, and the Commander, Air Force Reserve Command, (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **in accordance with Defense Information Systems Agency, "Access Control in Support of Information Systems," Security Technical Implementation Guide, Version 2, Release 3, October 29, 2010.**

(U) Management Comments Required

(U) The Commander, Air Force Materiel Command and Commander, Air Force Reserve Command did not provide comments to the draft report. Therefore, we request the Commanders provide comments in response to the final report.

(U) Recommendation A.3

~~(S)~~ We recommend that the Commander, U.S. Cyber Command and Director, Defense Information Systems Agency, coordinate to issue clarifying guidance for

~~(S)~~ the Task Order 14-0185, "Insider Threat Mitigation," July 17, 2014, to instruct DoD Components to (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]**.**

(U) U.S. Cyber Command Comments

~~(FOUO)~~ The U.S. Cyber Command, Deputy Director, Current Operations, agreed, stating that the existing Defense Information Systems Agency Device Control Module guidance will be updated to (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]. The Defense Information Systems Agency will work in coordination with U.S. Cyber Command to update the guidance and notify the community when released.

(U) Our Response

(U) Comments from the Deputy Director addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

(U) Defense Information Systems Agency Comments

~~(FOUO)~~ The Defense Information Systems Agency, Executive, Infrastructure Development, agreed, stating that the Defense Information Systems Agency Infrastructure Directorate will update the Device Control Module guidance to (b)(3), 10 USC § 130e, (b)(7) [redacted]. The Defense Information Systems Agency will work in coordination with U.S. Cyber Command to update the guidance and notify the community when released.

(U) Our Response

(U) Comments from the Executive addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

(U) Recommendation A.4

~~(FOUO)~~ We recommend that the Commander, Air Force Space Command, submit (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **to the Defense Information Systems Agency for** (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **in accordance with applicable DoD guidance, either**

~~(FOUO)~~ DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007 or DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014.

(U) Management Comments Required

(U) The Commander, Air Force Space Command did not provide comments to the draft report. Therefore, we request the Commander provide comments in response to the final report.

(U) Recommendation A.5

(U) We recommend the Air Force Chief, Information Dominance Chief Information Officer:

a. **~~(FOUO)~~ Review the deficiencies identified, require a thorough review of the Air Force Secret Internet Protocol Router Network security safeguards performed at each command, and apply corrective actions as necessary.**

(U) Air Force Information Dominance Chief Information Officer Comments

(U) The Air Force Information Dominance Chief Information Officer, Chief, Cybersecurity Division, neither agreed nor disagreed, stating that SAF/CIO A6 identified (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] In addition, the SAF/CIO A6 is working with the Secretary of the Air Force, Inspector General (SAF/IG) to develop an Air Force-wide mandatory inspection item for the second quarter FY 2016. Estimated completion of tasks is second quarter FY 2017.

(U) Our Response

~~(FOUO)~~ Comments from the Chief partially addressed the recommendation. We request that the Chief provide additional comments that address all report findings, not just (b) (3), 10 USC § 130e, (b) (7)(E) Also, provide comments that describe the implementation plan in response to the final report.

b. **~~(FOUO)~~ Develop a plan to create a list of mission critical systems, update the list periodically, and provide this information to the appropriate communications squadron and network personnel at each base.**

(U) Air Force Information Dominance Chief Information Officer Comments

(U) The Air Force Information Dominance Chief Information Officer, Chief, Cybersecurity Division, neither agreed nor disagreed, stating that DoD Instruction 8510.01 states that the DoD Component CIO (SAF/CIO A6) must make (b) (3), 10 USC § 130e, (b) (7)(E)

(U) Our Response

~~(FOUO)~~ Comments from the Chief did not address the specifics of the recommendation. We agree that mission criticality (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] However, if the system owner considers the system mission critical, it is (b) (3), 10 USC § 130e, (b) (7)(E) The decision to classify a system as mission critical (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] In addition, the CSs (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] Therefore, we request the SAF/CIO A6 provide additional comments in response to the final report.

(U) Recommendation A.6

~~(S)~~ We recommend that the Commander, 24th Air Force, in coordination with the Commander, (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] in accordance with DoD policy.

(U) Management Comments Required

(U) The Commander, 24th Air Force and Commander, (b) (7)(E) [redacted] did not provide comments to the draft report. Therefore, we request the Commanders provide comments in response to the final report.

(U) Recommendation A.7

(U) We recommend that the Commander, (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011 and Technical Manual Methods and Procedures, TO 00-33B-5004, "Access Control for Information Systems," December 19, 2012.

(U) Commander, (b) (7)(E) [redacted] Comments

~~(FOUO)~~ The Director of Operations, (b) (7)(E) [redacted], neither agreed nor disagreed, stating that Air Force Reserve Command (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] In addition, (b) (7)(E) [redacted] developed procedures to (b) (3), 10 USC § 130e, (b) (7)(E) [redacted].

(U) Our Response

(U) Comments from the Director addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

(U) Recommendation A.8

(U) We recommend that the Commander, (b) (7)(E):

a. **~~(S)~~ Develop procedures to (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E)**

b. **~~(S)~~ Develop procedures to (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) to their major commands and the Air Force Chief, Information Dominance Chief Information Officer.**

(U) Commander, (b) (7)(E) Comments

~~(S)~~ The Commander, (b) (7)(E), neither agreed nor disagreed, (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E)

(U) Our Response

~~(S)~~ Comments from the Commander did not address the specifics of the recommendations. The process described (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) Therefore, we request the Commander provide comments in response to the final report.

c. **~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011 and Technical Manual Methods and Procedures, TO 00-33B-5004, "Access Control for Information Systems," December 19, 2012.**

(U) Commander, (b) (7)(E) [redacted] Comments

(U) The Commander, (b) (7)(E) [redacted], neither agreed nor disagreed, stating that processes are now in place to (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]. It will be the member's responsibility to contact their Information System Security Officer or CSA [Client System Administrator] to (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

(U) Recommendation A.9

(U) We recommend that the Commander, (b) (7)(E) [redacted]:

a. **~~(S)~~ Develop procedures to (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]**

(U) Commander, (b) (7)(E) [redacted] Comments

~~(S)~~ The Commander, (b) (7)(E) [redacted], agreed, stating that procedures are being developed to (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

b. **~~(S)~~ Develop procedures to** (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **to their major commands and the Air Force Chief, Information Dominance Chief Information Officer.**

(U) Commander, (b) (7)(E) [redacted] *Comments*

~~(S)~~ The Commander, (b) (7)(E) [redacted], agreed, stating (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

c. **~~(FOUO)~~** (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, and Technical Manual Methods and Procedures, TO 00-33B-5004, "Access Control for Information Systems," December 19, 2012.**

(U) Commander, (b) (7)(E) [redacted] *Comments*

~~(S)~~ The Commander, (b) (7)(E) [redacted], agreed, stating that the process has been implemented.

(U) Our Response

~~(FOUO)~~ Comments from the Commander addressed all of the specifics of the recommendation. No further comments are required to the final report.

(U) Recommendation A.10

(U) We recommend the Commander, (b) (7)(E) [redacted]**:**

a. **~~(S)~~ Develop procedures to** (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted], [redacted]

b. **~~(S)~~ Establish and implement procedures to** (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

c. **~~(S)~~** (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

d. **~~(FOUO)~~ Develop and implement** (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **according to the Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, and Air Force Manual 33-282, "Computer Security," March 27, 2012, and if** (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] **cannot be developed, then coordinate with base communications squadrons and any other necessary parties to develop a** (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) Management Comments Required

(U) The Commander, (b) (7)(E) [redacted], did not provide comments to the draft report. Therefore, we request the Commander provide comments in response to the final report.

(U) Finding B

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E)

~~(FOUO)~~ The Air Force (b) (3), 10 USC § 130e; (b) (7)(E). Specifically:

- ~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) in accordance with applicable DoD and Air Force guidance.[42] This occurred because (b) (3), 10 USC § 130e; (b) (7)(E)
- ~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) This occurred because the Air Force (b) (3), 10 USC § 130e; (b) (7)(E)
- ~~(FOUO)~~ (b) (7)(E), did not properly approve SIPRNet user access forms. This occurred because the CSs did not have effective policies and procedures to approve SIPRNet access.
- ~~(FOUO)~~ Security personnel at (b) (7)(E), did not conduct NATO briefings for all personnel with SIPRNet access. This occurred because (b) (7)(E) security personnel did not understand the requirement and (b) (7)(E) security personnel were not aware of the requirement to have all personnel take the NATO briefing.

~~(FOUO)~~ (b) (7)(E):

- ~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E)

(U) [42] National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996 and Air Force System Security Instruction 7703, "Communications Security: Protected Distribution Systems," August 26, 2008.

- ~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]; and
- ~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] in accordance with DoD guidance.[44] The PDSs were alarmed as required; (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]. In addition, (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] For details of the PDS technical inspections performed, see Appendix E. (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(U) [43] A PDS is used to transmit unencrypted classified information through an area of lesser classification.

(U) [44] National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996.

(U) [45] Air Force System Security Instruction 7703, "Communications Security: Protected Distribution Systems," August 26, 2008.

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ Additionally, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] For certification letter details see Appendix E. According to Air Force guidance, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ This occurred because (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

[redacted] The Commander, (b) (7)(E) [redacted] should develop and implement a plan to (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. In addition, the Commander, (b) (7)(E) [redacted] should immediately (b) (3), 10 USC § 130e; (b) (7)(E) [redacted].

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] We requested a list of SIPRNet access points from (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(U) [46] (b) (7)(E) [redacted].

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ This occurred because (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ System Access Forms Were Not Appropriately Completed or Approved

~~(FOUO)~~ (b) (7)(E) [redacted], did not verify completion of required SIPRNet access forms. The Air Force requires each user who requests SIPRNet access to complete:

(U) [47] Enterprise Network Data Repository

- ~~(FOUO)~~ DD Form 2875, "System Authorization Access Request (SAAR)" in accordance with Air Force Manual 33-152, "User Responsibilities and Guidance for Information Systems," June 1, 2012. This form documents supervisor, security manager, and IAO approval for system access and need to know;
- ~~(FOUO)~~ DD Form 2842, "Department of Defense Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities," August 2009. This form is used to acknowledge the users responsibility to safeguard the token and the registration official verifies the identity of the individual;
- ~~(FOUO)~~ SF 312, "Nondisclosure Agreement" in accordance with Air Force Instruction 31-501, "Personnel Security Program Management," January 27, 2005. Users complete this form to accept the obligation to protect classified information; and
- ~~(FOUO)~~ Air Force (AF) Form 4394, "Air Force User Agreement Statement-Notice and Consent Provision" in accordance with Air Force Manual 33-152, "User Responsibilities and Guidance for Information Systems," June 1, 2012. This form identifies rules of system use and user consent to monitoring.

~~(FOUO)~~ The CSs did not verify completion of required forms to gain SIPRNet access. To determine if the forms required to gain access to SIPRNet were correctly completed, we performed control tests for the DD Forms 2875, DD Forms 2842, SF 312, and AF Forms 4394 for 45 personnel at (b) (7)(E) [redacted], and for 39 personnel at (b) (7)(E) [redacted]. We identified errors in the forms and, therefore, the control test failed. The Table below identifies the number of forms provided by the respective CS and outlines the results of our analysis.

(U) Table. Forms Required for SIPRNet Access

~~(FOUO)~~ (b) (7)(E) [redacted]	DD Form 2875	DD Form 2842	SF 312	AF Form 4394
Received (out of 45)	20	34	36	15
Completed Correctly	11	25	36	15
Completed Incorrectly	9	9	0	0
Forms Not Received	25	11	9	30
(b) (7)(E) [redacted]				
Received (out of 45)	22	44	41	20
Completed Correctly	16	44	41	20
Completed Incorrectly	6	0	0	0
Forms Not Received	23	1	4	25
(b) (7)(E) [redacted]				
Received (out of 39)	36	28	37	38
Completed Correctly	5	28	37	37
Completed Incorrectly	31	0	0	1
Forms Not Received	3	11	2	1

(U) Note: See Appendix F for more detail. ~~(FOUO)~~

~~(FOUO)~~ This occurred because the CSs did not establish policies and procedures to verify that all IAOs completed and approved forms required for network access before they provided users with SIPRNet access. (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

The Commander (b) (7)(E) [redacted]; the Commander, (b) (7)(E) [redacted]; and the Commander, (b) (7)(E) [redacted], should develop procedures to verify that access forms are accurately completed before access to the SIPRNet is granted.

~~(FOUO)~~ Air Force Did Not Conduct NATO Briefings

~~(FOUO)~~ Security personnel at (b) (7)(E) [redacted] did not conduct NATO briefings for all personnel with SIPRNet access. The security manager at (b) (7)(E) [redacted] stated that they provided the NATO briefing within a Security Administration briefing; however there was not written acknowledgement of the briefings as required by Air Force guidance. The security managers at (b) (7)(E) [redacted] stated that they only provided the briefings when access to NATO information was necessary. However, NATO information is not segmented on SIPRNet and (b) (7)(E) [redacted]

~~(FOUO)~~ (b) (7)(E) [redacted]. According to DoD[48] and Air Force Guidance,[49] all cleared military, civilian, and contractor personnel should receive a NATO security briefing and a written acknowledgement of the NATO training will be maintained.

~~(FOUO)~~ This occurred because the (b) (7)(E) [redacted] security personnel were not sure what "all cleared personnel" meant. Additionally, security personnel at (b) (7)(E) [redacted] thought a read receipt would satisfy the requirement for written acknowledgement. Finally, security personnel at (b) (7)(E) [redacted] were not aware of the requirement to have all personnel take the NATO briefing. The requirement for NATO briefings is important due to the ongoing missions and operations of the Air Force. Since NATO briefings were not conducted, individuals were not aware of the appropriate method to secure and protect NATO information. The Administrative Assistant to the Secretary of the Air Force, should develop an action plan to ensure Air Force commands conduct the NATO briefings for all personnel as required by DoD Manual 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, and develop a mechanism to identify and track personnel who receive the training.

~~(FOUO)~~ Since NATO briefings were not conducted, individuals were not aware of the appropriate method to secure and protect NATO information.

(U) [48] DoD Manual 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012.

(U) [49] Air Force Instruction 31-401, "Information Security Program Management," Change 1, August 19, 2009 was in effect when we began the audit. However, during the audit it was superseded by Air Force Instruction 16-1404, "Air Force Information Security Program," May 29, 2015.

~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ The physical safeguards for the Air Force SIPRNet (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

~~(FOUO)~~ DoD must defend its information and must do more to secure its cyber infrastructure. The physical safeguards for the Air Force SIPRNet (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation B.1

~~(FOUO)~~ The Administrative Assistant to the Secretary of the Air Force, should develop an action plan to ensure Air Force commands conduct the North Atlantic Treaty Organization briefings for all personnel as required by DoD Manual 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, and develop a mechanism to identify and track personnel who receive the training.

(U) Administrative Assistant to the Secretary of the Air Force Comments

(U) We received the Administrative Assistant to the Secretary of the Air Force comments on the draft report too late to include them in the final report. Therefore, if the Administrative Assistant to the Secretary of the Air Force does not submit additional comments, we will consider those comments as the management response to the final report.

(U) Recommendation B.2

~~(FOUO)~~ We recommend that the Air Force Chief, Information Dominance Chief Information Officer, determine a (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

(U) Air Force Chief, Information Dominance Chief Information Officer Comments

~~(FOUO)~~ The Air Force Information Dominance Chief Information Officer, Chief, Cybersecurity Division, neither agreed nor disagreed, stating that there is a policy in place and units were notified on July 6, 2010. The policy is the Methods and Procedures Technical Manual 00-33d-2001, "Active Directory Naming Conventions," May 8, 2009. The Manual provides instructions for entry into Active Directory with standard naming convention to include physical location and designated system administrator. The SAF/CIO A6 recommends CS reference equipment location in Active Directory and ensure adherence to the Active Directory Naming Conventions. In addition, Air Force Manual 33-153, "Information Technology Management," provides guidance to manage Air Force equipment.

(U) Our Response

~~(FOUO)~~ Comments from the Chief did not address the specifics of the recommendation. The Air Force Manual and Methods and Procedures Technical Manual described do not require (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]. Therefore, we request the SAF/CIO A6 provide comments in response to the final report.

(U) Recommendation B.3

~~(FOUO)~~ We recommend that the Commander, (b)(7)(E) [redacted] **develop procedures to verify that access forms are accurately completed before access is granted to the Secret Internet Protocol Router Network.**

(U) Commander, (b) (7)(E) [redacted] *Comments*

(U) The Director of Operations, (b) (7)(E) [redacted] CS, neither agreed nor disagreed, stating that the (b) (7)(E) [redacted] CS has implemented a process to ensure completion and standardization of the DD Form 2875. This process involves the participation of the requestor's supervisor, unit security manager, and unit IAO. A form submitted will be reviewed for accuracy by the Information Assurance Manager, Local Registration Authority, and SIPRNet Client Service Technician. The DD Form 2875 will be returned to the unit IAO if received incomplete. The requestor will provide copies of their derivative training and Cyber Awareness training certificates.

(U) Our Response

(U) Comments from the Director addressed all of the specifics of the recommendation. No further comments are required to the final report; however, we request a copy of the formal policies and procedures described in the management comments before this recommendation can be closed.

(U) Recommendation B.4

(U) We recommend that the Commander, (b) (7)(E) [redacted]**:**

a. **~~(FOUO)~~ Develop and implement a plan to** (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]**.**

b. **~~(FOUO)~~ Immediately** (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]**.**

c. **~~(FOUO)~~** (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] **as required by Air Force System Security Instruction 7703, "Communications Security: Protected Distribution Systems," August 26, 2008.**

(U) Commander, (b) (7)(E) [redacted] *Comments*

(U) The Commander, (b) (7)(E) [redacted] CS, neither agreed nor disagreed, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation. No further comments are required to the final report.

d. ~~**(FOUO)**~~ **Develop procedures to verify that access forms are accurately completed before access is granted to the Secret Internet Protocol Router Network.**

(U) Commander, (b)(7)(E) [redacted] Comments

~~(FOUO)~~ The Commander, (b)(7)(E) [redacted] CS, neither agreed nor disagreed, stating that processes are currently in place to ensure that all documents are properly filled out before submitting a SIPRNet account request by the unit Information Systems Security Officer. This has been briefed to squadron, group, and wing commanders.

(U) Our Response

(U) Comments from the Commander did not address the specifics of the recommendation. The process described was not effective as discussed in the report. (b)(7)(E) [redacted] could not provide 75 access forms and users did not properly complete 18 access forms. Therefore, we request the Commander provide comments in response to the final report.

(U) Recommendation B.5

~~**(FOUO)**~~ **We recommend that the Commander, (b)(7)(E) [redacted] develop procedures to verify that access forms are accurately completed before access is granted to the Secret Internet Protocol Router Network.**

(U) Commander, (b)(7)(E) [redacted] Comments

~~(FOUO)~~ The Commander, (b)(7)(E) [redacted] Mission Support Group, agreed, stating that (b)(7)(E) [redacted] follows Air Force Network procedures for account creation and paperwork in accordance with Air Force Manual 33-282. The Unit CSL maintains and provides the CS a copy of the DD Form 2875 to review for proper signatures before accounts are created. The regulation requires the unit CSL to maintain the original paperwork.

(U) Our Response

(U) Comments from the Commander did not address the specifics of the recommendation. The process described was not effective as discussed in the report. (b) (7)(E) could not provide 53 access forms and users did not properly complete 6 access forms. Therefore, we request the Commander provide comments in response to the final report.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from October 2014 through July 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We performed the audit to determine whether the Air Force effectively protected SIPRNet access points. We focused our review on the Air Force SIPRNet managed by (b)(7)(E) [redacted]. We nonstatistically selected a sample of three Air Force bases ((b)(7)(E) [redacted]) to determine whether Air Force commands properly implemented logical and physical controls to protect SIPRNet access points. The commands chosen represented SIPRNet use that varied among active military and reserves. We reviewed physical and logical security safeguards at each base and logical controls at (b)(7)(E) [redacted] and (b)(7)(E) [redacted]. In addition, we reviewed the certification and accreditation packages for each base.

(U) During our review, we interviewed DoD and Air Force component personnel. We interviewed personnel at:

- (U) U.S. Cyber Command to discuss (b)(3), 10 USC § 130e, (b)(7)(E) [redacted];
- (U) SAF/CIO A6 to discuss SIPRNet (b)(3), 10 USC § 130e, (b)(7)(E) [redacted];
- (U) (b)(7)(E) [redacted] and (b)(7)(E) [redacted] to obtain, review, and analyze (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]; and
- (U) (b)(3), 10 USC § 130e, (b)(7)(E) [redacted], and required security training. In addition, we:
    - (U) obtained, reviewed, and analyzed local policies;

- (U) obtained, reviewed, and analyzed network access and write privilege processes;
- (U) obtained, reviewed, and analyzed vulnerability management, user authentication, account monitoring, asset management, and personnel access policies and procedures; and
- (U) observed physical security for SIPRNet access points.

(U) In addition, we performed control tests for:

- (U) write privileges;
- (U) background checks; and
- (U) DD Forms 2875, DD Forms 2842, SF 312, and AF Forms 4394.

(U) We selected a random[50] sample of:

- (U) 45 accounts from a universe of (b)(7)(E) SIPRNet accounts at (b)(7)(E) ;
- (U) 45 accounts from a universe of (b)(7)(E) SIPRNet accounts at (b)(7)(E) ; and
- (U) 39 accounts from a universe of (b)(7)(E) SIPRNet accounts at (b)(7)(E) .

(U) These decision rules applied for our control tests: if there were no errors in the sample, then the control passed, and if there were one or more errors, then the control failed. We used the control test table developed by Quantitative Methods Division at the DoD OIG and published in the Council of the Inspectors General on Integrity and Efficiency, "Journal of Public Inquiry," 2012-2013.

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E)

[50] (U) We selected a nonstatistical sample of user accounts. We randomized the universe to reduce bias during the sample selection.

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted].

(U) To determine whether the DD Forms 2875 were appropriately completed and approved, we verified if the:

- (U) user, information assurance officer, and security manager signed the form;
- (U) IA training was completed within a year of the information assurance manger's signature; and
- (U) boxes were checked to annotate the user had a need to know and access to classified information.

(U) To determine whether DD Forms 2842 were appropriately completed and approved, we verified that the user and registration official signed and dated the form. Finally, to determine whether the AF Forms 4394 were appropriately completed, we verified that the user signed and dated the forms.

(U) In addition, to determine whether (b) (3), 10 USC § 130e, (b) (7)(E) [redacted], we requested a list of users (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] during the 6-month period from August 2014 through January 2015 from (b) (7)(E) [redacted], to compare to a list of current SIPRNet users.

(U) Use of Computer-Processed Data

~~(FOUO)~~ We obtained and analyzed certification and accreditation packages from Enterprise Mission Assurance Support Service. We used the packages to determine whether the SIPRNet accreditation at the Air Force bases was appropriate. To assess the reliability of the Enterprise Mission Assurance Support Service accreditation data, we compared the data to controls in operation. In addition, we interviewed Air Force and Defense Information Systems Agency personnel on the data accuracy. (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] as discussed in Finding A.

~~(FOUO)~~ We obtained and analyzed Assured Compliance Assessment Solution vulnerability scans from (b)(7)(E) [redacted]. We used the data to determine if (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]. Assured Compliance Assessment Solution is a DoD tool managed by Defense Information Systems Agency. (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] We interviewed the SAF/CIO A6, (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] identified in the vulnerability scans. We determined that these documents were sufficiently reliable for the purpose of this report.

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted], as discussed in Finding B.

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted], as discussed in Finding A.

~~(FOUO)~~ We obtained and analyzed data from the Joint Personnel Adjudication System. The data was used to determine if personnel received background checks and signed nondisclosure agreements. Joint Personnel Adjudication System is the official repository of security information for DoD and the Defense Manpower Data Center manages the system. We interviewed security managers about the data stored in the Joint Personnel Adjudication System and observed them query the data. We determined that this data were sufficiently reliable for the purpose of this report.

(U) Use of Technical Assistance

(U) We obtained support from the DoD OIG Quantitative Methods Division to develop a random sample for review. We obtained support from the DoD OIG Technical Assessment Directorate to define SIPRNet access points.

(U) Prior Coverage

(U) During the last 5 years, the Air Force Audit Agency issued one report discussing controlled access to universal serial bus ports and compact disk drives and mitigation of identified vulnerabilities.

(U) Air Force Audit Agency

~~(S)~~ F2015-0002-030000, "Classified Information Systems Protection – Secret Internet Protocol Router Network," February 10, 2015.

(U) Appendix B

(U) DoD Information Assurance Certification and Accreditation Process

(U) The DIACAP establishes a process to certify and accredit DoD information systems based on the implementation of IA controls. DIACAP applies to all DoD-owned and controlled information systems and consists of five activities:

(U) Activity 1: Initiate Certification and Accreditation. Register the system with the appropriate DoD Component, assign IA controls to the information system, and initiate the DIACAP Implementation Plan. Each assigned control is implemented according to the applicable implementation guidelines provided in the DIACAP.

(U) Activity 2: Implement and Validate IA Controls. Executes the DIACAP Implementation Plan, conducts validation activities, prepares the IT Security POA&M, and compiles validation results in the DIACAP Scorecard. The status of each assigned IA control is indicated on the DIACAP Scorecard as compliant, noncompliant, or not applicable.

(U) Activity 3: Make Certification Determination and Accreditation Decision. Determines whether to certify and accredit a DoD information system. Each information system has a certifying authority, who bases the certification decision on IA validation results, and a designated accrediting authority, who bases the accreditation decision on a balance of mission or business need and protection of the information being processed.

(U) Activity 4: Maintain Authorization. Sustains acceptable IA posture. The IA controls should be reviewed annually to confirm the effectiveness of the assigned IA controls or to recommend changes to the accreditation status. A designated accrediting authority may downgrade or revoke an accreditation decision at any time if risk conditions or concerns develop from the reviews. The results of an annual review or a major change in information assurance posture at any time may indicate the need for recertification and reaccreditation.

(U) Activity 5: Decommissioning. Removes DoD information system from operation.

(U) Appendix C

~~(FOUO)~~ (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(~~S~~) We requested and reviewed the vulnerability scans (b) (1), 1.4(g), (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

~~(FOUO)~~ Table. (b) (3), 10 USC § 130e, (b) (7)(E) [redacted]

(~~S~~) Location	November	December	January	February	March
(b) (1), 1.4(g) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
					(~~S~~)

(U) Appendix D

(U) Test Results for (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

~~(FOUO)~~ We compared lists of personnel (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] from August 2014 through January 2015 provided by (b)(7)(E) [redacted], and (b)(7)(E) [redacted], to a list of SIPRNet users (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] In addition, while performing other control tests, we identified users (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]; therefore, we did not perform a control test for (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] However, while performing other control tests, we identified (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] The Table below identifies the sites tested and identifies the results of the analysis including the number of (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]

(U) Table. (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] *Discovered During Testing*

~~(FOUO)~~ Sites Tested	(b)(3), 10 USC § 130e, (b)(7)(E) [redacted]		
(b)(7)(E) [redacted]	Not Provided	(b)(3), 10 USC § 130e, (b)(7)(E) [redacted]	
(b)(7)(E) [redacted]	(b)(3), 10 USC § 130e, (b)(7)(E) [redacted]		N/A
(b)(7)(E) [redacted]			N/A
			~~(FOUO)~~

(U) Appendix E

(U) Test Results for Protected Distribution Systems

~~(FOUO)~~ We requested [redacted] certification letters and PDS technical inspections. We received and reviewed [redacted] certification letters and [redacted] technical inspection documents. Our analysis of (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] identified:

- ~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~

(U) Our analysis of the [redacted] that had evidence of a technical inspection identified:

- ~~(FOUO)~~ (b)(3), 10 USC § 130e, (b)(7)(E) [redacted]
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~

(U) Appendix F

(U) Control Test Results for Forms Required for System Access

(U) (b) (7)(E) [redacted]

(U) DD Form 2875

~~(FOUO)~~ At (b) (7)(E) [redacted], we received and reviewed 20 of the 45 requested DD Forms 2875. Of the 20 forms reviewed, 9 were not completed correctly including some with multiple discrepancies. Specifically,

- ~~(FOUO)~~ 2 were signed and approved after we requested them from (b) (7)(E) [redacted] CS;
- ~~(FOUO)~~ 3 personnel did not meet the annual requirement for IA training before signing the form;
- ~~(FOUO)~~ 1 was not signed and approved by the IAO; and
- ~~(FOUO)~~ 5 did not have properly filled out access and need to know requirements; specifically, 2 of the 5 did not indicate the user had a "need to know" and 3 of the 5 did not indicate the user needed access to classified information.

~~(FOUO)~~ (b) (7)(E) [redacted] could not provide 25 of the 45 DD Forms 2875.

(U) DD Form 2842

~~(FOUO)~~ We received and reviewed 34 of the 45 requested DD Forms 2842. Of the 34 forms reviewed, 9 did not have the required user or IAO signatures. (b) (7)(E) [redacted] could not provide 11 of the 45 DD Forms 2842.

(U) SF Form 312

~~(FOUO)~~ We received and reviewed 36 of the 45 requested SF Forms 312 and all were completed correctly. (b) (7)(E) [redacted] did not provide 8 of the 45 SF Forms 312 because the (b) (7)(E) [redacted] Chief, Information Protection, stated that the eight individuals had left (b) (7)(E) [redacted]. They could not provide 1 of the 45 SF Forms 312.

(U) AF Form 4394

~~(FOUO)~~ We received and reviewed 15 of the 45 requested AF Forms 4394 and all were completed correctly. (b)(7)(E) [redacted] could not provide 30 of the 45 AF Forms 4394.

(U) (b)(7)(E) [redacted]

(U) DD Form 2875

~~(FOUO)~~ At (b)(7)(E) [redacted], we received and reviewed 22 of the 45 requested DD Forms 2875. Of the 22 forms reviewed, 6 were not completed correctly including some forms with multiple discrepancies. Specifically,

- ~~(FOUO)~~ 2 were not signed by the information owner or IAO;
- ~~(FOUO)~~ 2 were not signed by the security manager; and
- ~~(FOUO)~~ 5 did not indicate that the user had a need to know.

~~(FOUO)~~ (b)(7)(E) [redacted] did not provide 23 of the 45 DD Forms 2875 for various reasons such as users had left the base, confusion in the process for granting access, or an error in processing.

(U) DD Form 2842

~~(FOUO)~~ We received and reviewed 44 of the 45 requested DD Forms 2842 and all were completed correctly. (b)(7)(E) [redacted] did not provide 1 of the 45 DD Forms 2842 because the (b)(7)(E) [redacted] created an account for a user that never came to complete the DD Form 2842 before leaving (b)(7)(E) [redacted].

(U) SF Form 312

~~(FOUO)~~ We received and reviewed 41 of the 45 requested SF Forms 312 and all were completed correctly. (b)(7)(E) [redacted] was unable to provide SF 312s for 4 of the 45 users.

(U) AF Form 4394

~~(FOUO)~~ We received and reviewed 20 of the 45 requested AF Forms 4394 and all were completed correctly. (b)(7)(E) [redacted] did not provide 25 of the 45 AF Forms 4394 for various reasons such as users had left the base, confusion in the process for granting access, or an error in processing.

(U) (b) (7)(E)

(U) DD Form 2875

~~(FOUO)~~ At (b) (7)(E), we received and reviewed 36 of the 39 requested DD Forms 2875. (b) (7)(E) did not provide 3 of the 39 DD Forms 2875 because the (b) (7)(E) Information Assurance Manager stated that until December 2014, (b) (7)(E) did not have an established Information Assurance Officer program to ensure completion of the DD Forms 2875. Of the 36 DD forms reviewed, 31 were not completed correctly including some forms with multiple discrepancies.

- ~~(FOUO)~~ 1 did not have the Security Manager's approval of security clearance;
- ~~(FOUO)~~ 2 did not have correct IA training documented; specifically, one person did not have IA training noted on the form and one person did not have IA training before signing the form and gaining access to the SIPRNet;
- ~~(FOUO)~~ 30 were not signed and approved by the IAO; and
- ~~(FOUO)~~ 12 did not have properly filled out access and need to know requirements. Specifically, of the 12:
  - ~~(FOUO)~~ 2 did not have "need to know" or access to classified information checked on the form,
  - ~~(FOUO)~~ 4 did not have "need to know" checked on the form, and
  - ~~(FOUO)~~ 6 did not have access to classified information checked on the form.

(U) DD Form 2842

~~(FOUO)~~ We received and reviewed 37 of the 39 requested DD Forms 2842 and all were completed correctly. (b) (7)(E) did not provide 2 of the 39 DD Forms 2842 because the (b) (7)(E) Information Assurance Manager stated that they misplaced the forms.

(U) SF Form 312

~~(FOUO)~~ We received and reviewed 37 of the 39 requested SF Forms 312 and all were completed correctly. (b) (7)(E) did not provide 2 of the 39 SF Forms 312 because the (b) (7)(E) Chief, Information Protection, stated that the two individuals had left (b) (7)(E)

(U) AF Form 4394

~~(FOUO)~~ We received and reviewed 38 of the 39 requested AF Forms 4394 and one was not completed correctly. (b) (7)(E) did not provide 1 of the 39 AF Forms 4394 because the (b) (7)(E) Information Assurance Manager stated that until December 2014, (b) (7)(E) did not have an established Information Assurance Officer program to ensure completion of the AF Forms 4394.

(U) Appendix G

(U) Criteria

(U) We used the following guidance throughout the audit.

(U) National Security Telecommunications and Information Systems Security Committee

(U) National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996, outlines the approval authority, standards, and guidance for PDS design, installation, and maintenance.

(U) Chairman of the Joint Chiefs of Staff

(U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, provides joint policy and responsibilities for IA and support to computer network defense.

(U) DoD

(U) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other Federal agencies, for the authorization and connection of information systems.

(U) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, establishes a certification and accreditation process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD information systems.

(U) DoD Manual 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, implements policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information and classified information.

(U) Office of the Secretary of Defense Memorandum "Insider Treat Mitigation," July 12, 2013, provides procedures for information protection and insider threat mitigation to all DoD Components.

(U) U.S. Cyber Command

~~(FOUO)~~ U.S. Cyber Command Task Order 14 0185, "Insider Threat Mitigation," July 17, 2014, implements a number of technical and procedural safeguards to mitigate vulnerabilities exploitable by a determined insider threat.

(U) Air Force

(U) Air Force Instruction 16-1404, "Air Force Information Security Program," May 29, 2015, supersedes Air Force Instruction 31-401 and explains how to manage and protect unclassified controlled information and classified information.

(U) Air Force Instruction 31-401, "Information Security Program Management," Change 1, August 19, 2009, explains how to manage and protect unclassified controlled information and classified information.

(U) Air Force Instruction 31-501, "Personnel Security Program Management," dated January 27, 2005, provides guidance for personnel security investigations and clearance needs.

(U) Air Force Manual 33-152, "User Responsibilities and Guidance for Information Systems," dated June 1, 2012, identifies policies and procedures for the use of cyberspace support systems and services and compliance requirements.

(U) Air Force Manual 33-282, "Computer Security," March 27, 2012, implements computer security, which is designed to ensure the employment of countermeasures to protect and secure US government information processed by Air Force information systems by protecting the confidentiality, integrity, availability, authentication, and non-repudiation of information systems.

(U) Air Force System Security Instruction 7703, "Communications Security: Protected Distribution Systems," August 26, 2008, provides the minimum protection standards based on national guidance for PDS to ensure the PDS provides adequate electrical, electromagnetic, physical, and procedural safeguards.

(U) Defense Information Systems Agency

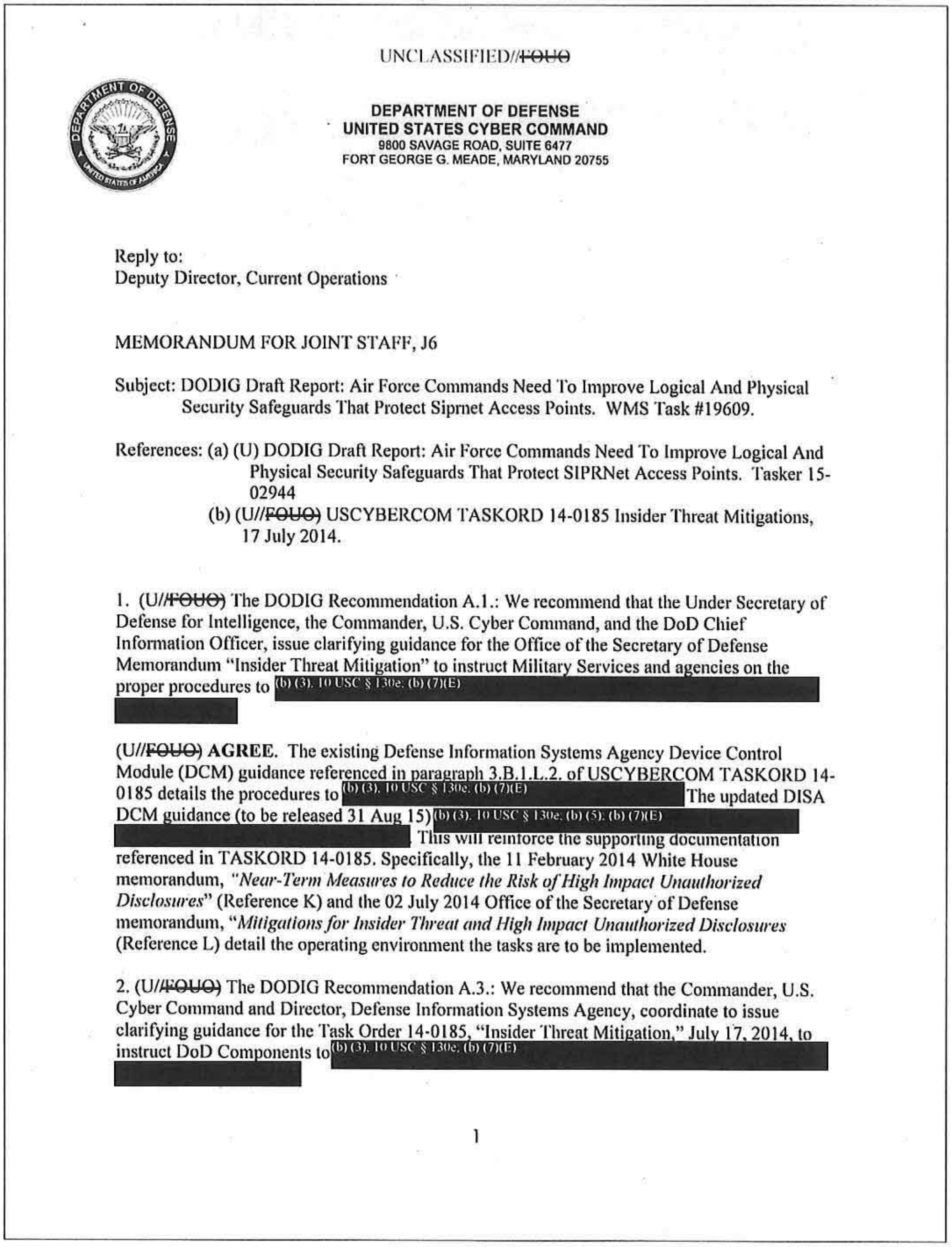
(U) Defense Information Systems Agency "Enclave" Security Technical Implementation Guide, Version 4, Release 4, January 9, 2014, provides assistance in meeting the minimum requirements, standards, controls, and options for securing an enclave as a whole and providing the technical guidance to secure specific enclave components in detail.

(U) Defense Information Systems Agency, "Access Control in Support of Information Systems," Security Technical Implementation Guide, Version 2, Release 3, October 29, 2010, provides details for security framework for use when planning and selecting access control for protecting sensitive and classified information in DoD. It provides background and context for access control issues including the process of identification, authentication, and authorization for access to protected assets.

(U) Defense Information Systems Agency, Program Executive Office – Mission Assurance, Host Based Security System, "Device Control Module Guidance for Task Order 14-0185," October 28, 2014, provides directorate level instructions for restricting the use of removable media on systems across the DoD.

(U) Management Comments

(U) U.S. Cyber Command



UNCLASSIFIED//~~FOUO~~

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

Reply to:
Deputy Director, Current Operations

MEMORANDUM FOR JOINT STAFF, J6

Subject: DODIG Draft Report: Air Force Commands Need To Improve Logical And Physical Security Safeguards That Protect Siprnet Access Points. WMS Task #19609.

References: (a) (U) DODIG Draft Report: Air Force Commands Need To Improve Logical And Physical Security Safeguards That Protect SIPRNet Access Points. Tasker 15-02944
(b) (U//~~FOUO~~) USCYBERCOM TASKORD 14-0185 Insider Threat Mitigations, 17 July 2014.

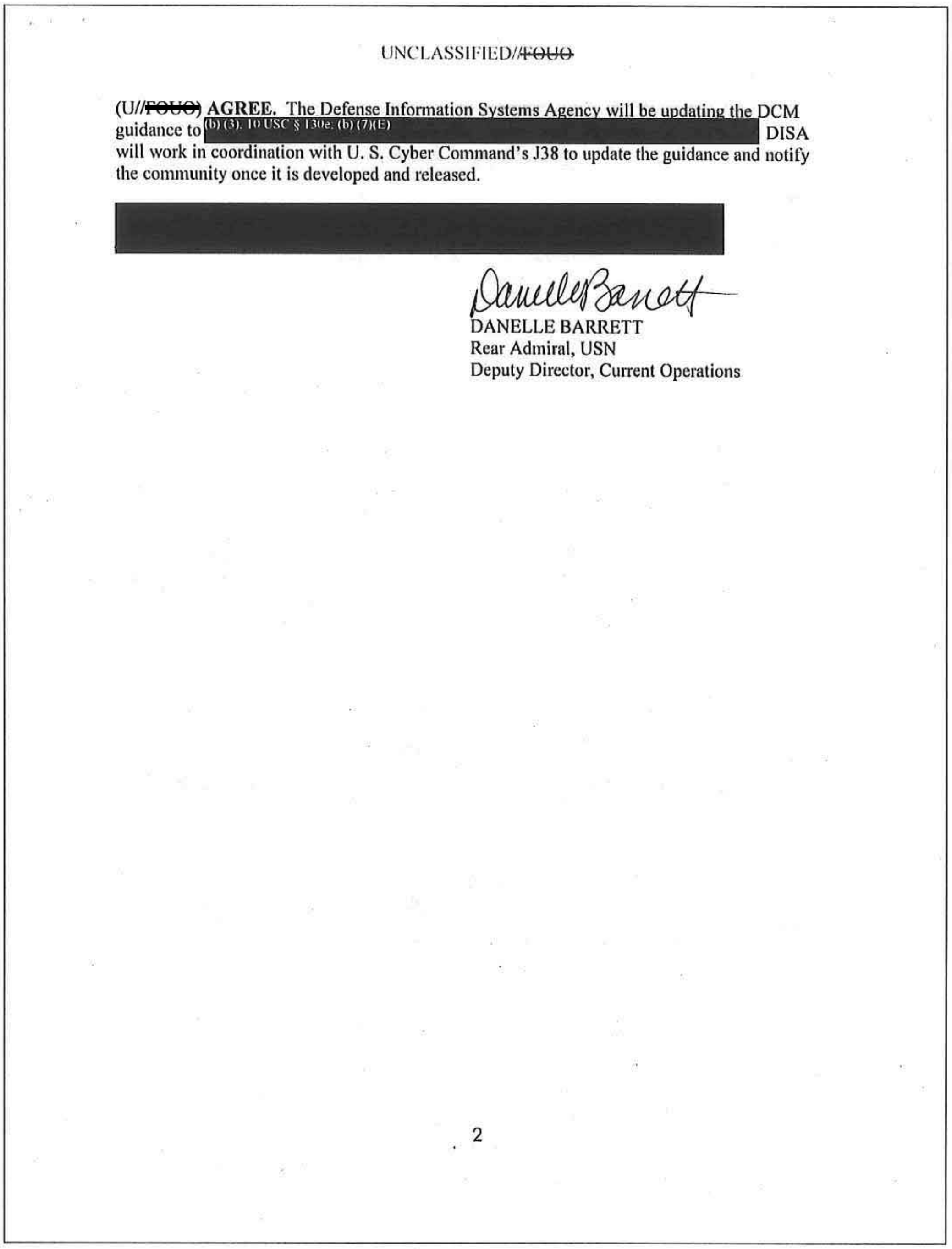
1. (U//~~FOUO~~) The DODIG Recommendation A.1.: We recommend that the Under Secretary of Defense for Intelligence, the Commander, U.S. Cyber Command, and the DoD Chief Information Officer, issue clarifying guidance for the Office of the Secretary of Defense Memorandum "Insider Threat Mitigation" to instruct Military Services and agencies on the proper procedures to (b) (3), 10 USC § 130e, (b) (7)(E)

(U//~~FOUO~~) **AGREE.** The existing Defense Information Systems Agency Device Control Module (DCM) guidance referenced in paragraph 3.B.1.L.2. of USCYBERCOM TASKORD 14-0185 details the procedures to (b) (3), 10 USC § 130e, (b) (7)(E) The updated DISA DCM guidance (to be released 31 Aug 15) (b) (3), 10 USC § 130e, (b) (5), (b) (7)(E). This will reinforce the supporting documentation referenced in TASKORD 14-0185. Specifically, the 11 February 2014 White House memorandum, *"Near-Term Measures to Reduce the Risk of High Impact Unauthorized Disclosures"* (Reference K) and the 02 July 2014 Office of the Secretary of Defense memorandum, *"Mitigations for Insider Threat and High Impact Unauthorized Disclosures* (Reference L) detail the operating environment the tasks are to be implemented.

2. (U//~~FOUO~~) The DODIG Recommendation A.3.: We recommend that the Commander, U.S. Cyber Command and Director, Defense Information Systems Agency, coordinate to issue clarifying guidance for the Task Order 14-0185, "Insider Threat Mitigation," July 17, 2014, to instruct DoD Components to (b) (3), 10 USC § 130e, (b) (7)(E)

1

(U) U.S. Cyber Command (cont'd)



UNCLASSIFIED//~~FOUO~~

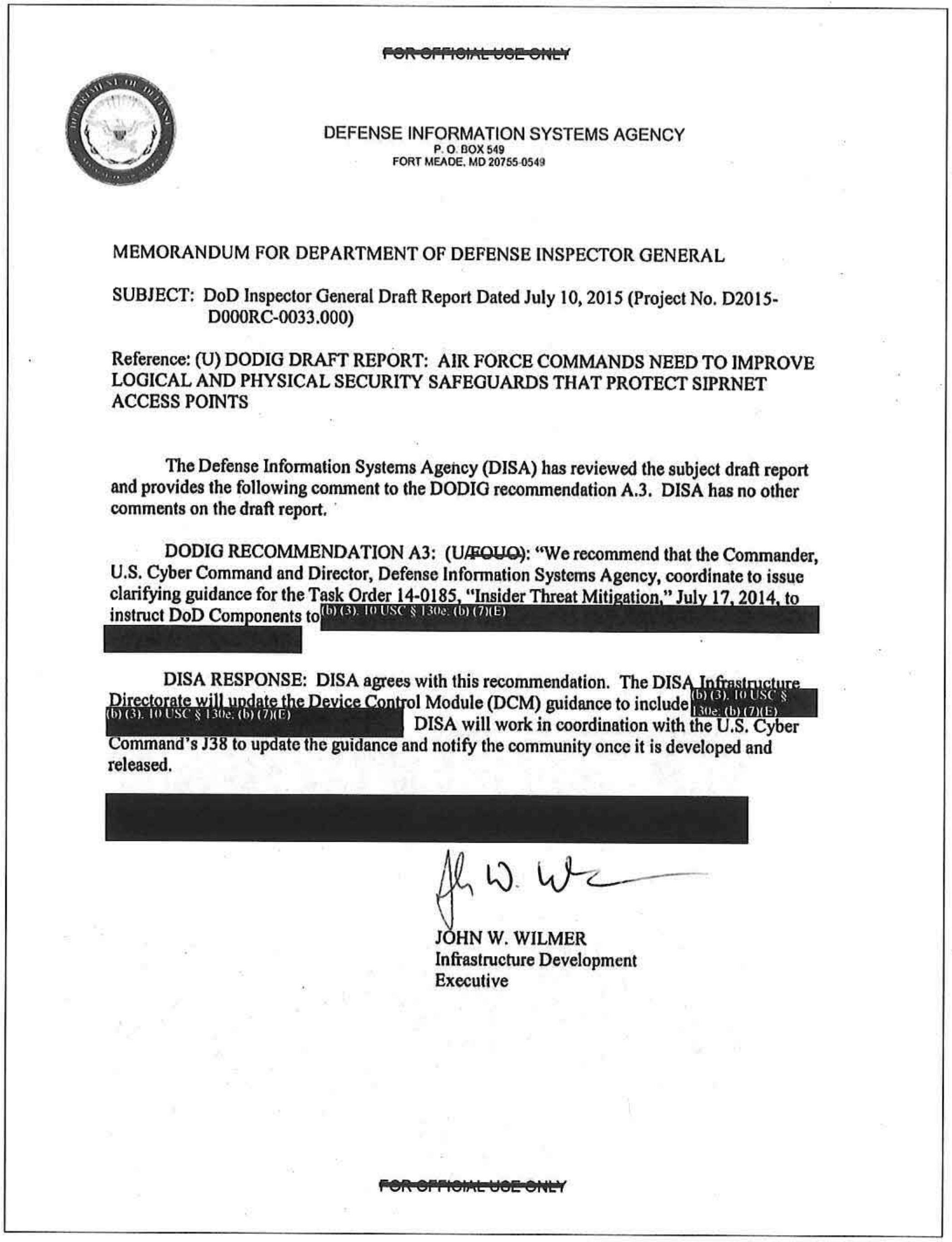
(U//~~FOUO~~) **AGREE.** The Defense Information Systems Agency will be updating the DCM guidance to (b)(3), 10 USC § 130e, (b)(7)(E) DISA will work in coordination with U. S. Cyber Command's J38 to update the guidance and notify the community once it is developed and released.

[redacted]

Danelle Barrett
DANELLE BARRETT
Rear Admiral, USN
Deputy Director, Current Operations

2

(U) Defense Information Systems Agency



~~FOR OFFICIAL USE ONLY~~

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MD 20755-0549

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: DoD Inspector General Draft Report Dated July 10, 2015 (Project No. D2015-D000RC-0033.000)

Reference: (U) DODIG DRAFT REPORT: AIR FORCE COMMANDS NEED TO IMPROVE LOGICAL AND PHYSICAL SECURITY SAFEGUARDS THAT PROTECT SIPRNET ACCESS POINTS

The Defense Information Systems Agency (DISA) has reviewed the subject draft report and provides the following comment to the DODIG recommendation A.3. DISA has no other comments on the draft report.

DODIG RECOMMENDATION A3: (U/~~FOUO~~): "We recommend that the Commander, U.S. Cyber Command and Director, Defense Information Systems Agency, coordinate to issue clarifying guidance for the Task Order 14-0185, "Insider Threat Mitigation," July 17, 2014, to instruct DoD Components to (b) (3), 10 USC § 130e, (b) (7)(E)

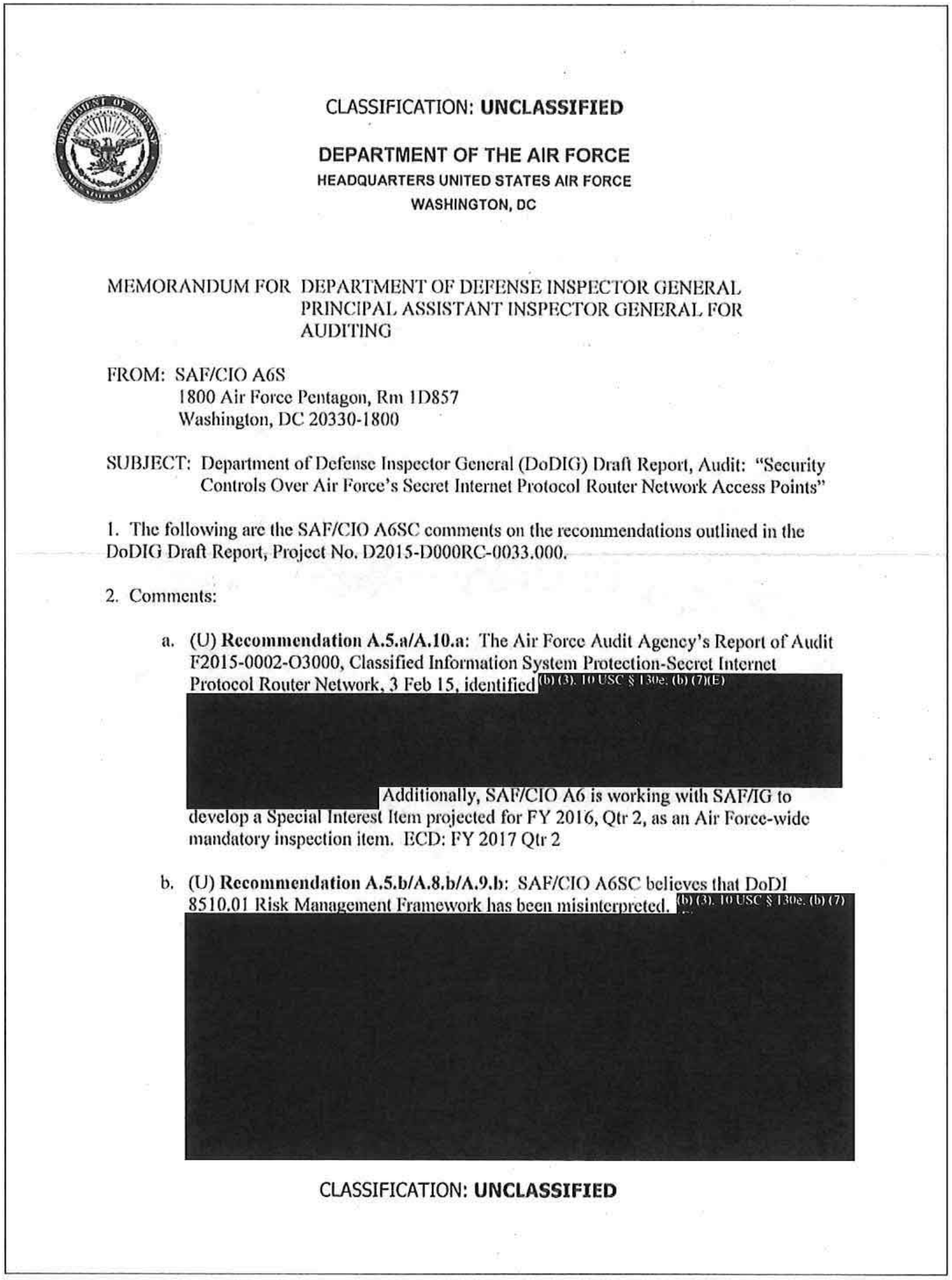
DISA RESPONSE: DISA agrees with this recommendation. The DISA Infrastructure Directorate will update the Device Control Module (DCM) guidance to include (b) (3), 10 USC § 130e, (b) (7)(E) DISA will work in coordination with the U.S. Cyber Command's J38 to update the guidance and notify the community once it is developed and released.

[redacted]

JOHN W. WILMER
Infrastructure Development
Executive

~~FOR OFFICIAL USE ONLY~~

(U) Air Force Chief, Information Dominance Chief Information Officer



CLASSIFICATION: **UNCLASSIFIED**

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL
PRINCIPAL ASSISTANT INSPECTOR GENERAL FOR
AUDITING

FROM: SAF/CIO A6S
1800 Air Force Pentagon, Rm 1D857
Washington, DC 20330-1800

SUBJECT: Department of Defense Inspector General (DoDIG) Draft Report, Audit: "Security Controls Over Air Force's Secret Internet Protocol Router Network Access Points"

1. The following are the SAF/CIO A6SC comments on the recommendations outlined in the DoDIG Draft Report, Project No. D2015-D000RC-0033.000.

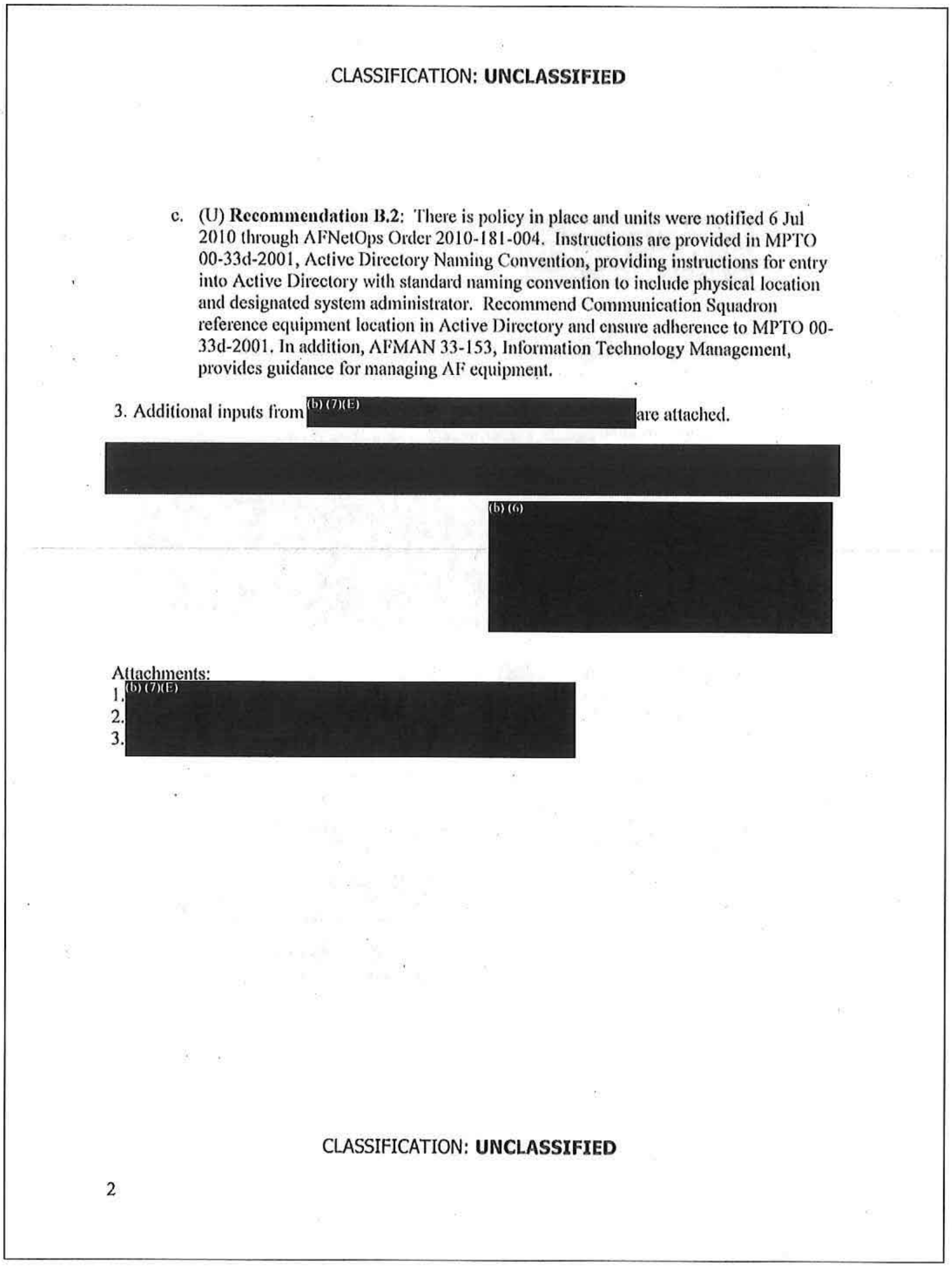
2. Comments:

a. (U) **Recommendation A.5.a/A.10.a**: The Air Force Audit Agency's Report of Audit F2015-0002-O3000, Classified Information System Protection-Secret Internet Protocol Router Network, 3 Feb 15, identified (b) (3), 10 USC § 130e, (b) (7)(E) [redacted] Additionally, SAF/CIO A6 is working with SAF/IG to develop a Special Interest Item projected for FY 2016, Qtr 2, as an Air Force-wide mandatory inspection item. ECD: FY 2017 Qtr 2

b. (U) **Recommendation A.5.b/A.8.b/A.9.b**: SAF/CIO A6SC believes that DoDI 8510.01 Risk Management Framework has been misinterpreted. (b) (3), 10 USC § 130e, (b) (7) [redacted]

CLASSIFICATION: **UNCLASSIFIED**

(U) Air Force Chief, Information Dominance Chief Information Officer (cont'd)



CLASSIFICATION: **UNCLASSIFIED**

c. (U) **Recommendation B.2**: There is policy in place and units were notified 6 Jul 2010 through AFNetOps Order 2010-181-004. Instructions are provided in MPTO 00-33d-2001, Active Directory Naming Convention, providing instructions for entry into Active Directory with standard naming convention to include physical location and designated system administrator. Recommend Communication Squadron reference equipment location in Active Directory and ensure adherence to MPTO 00-33d-2001. In addition, AFMAN 33-153, Information Technology Management, provides guidance for managing AF equipment.

3. Additional inputs from (b) (7)(E) [redacted] are attached.

[redacted]

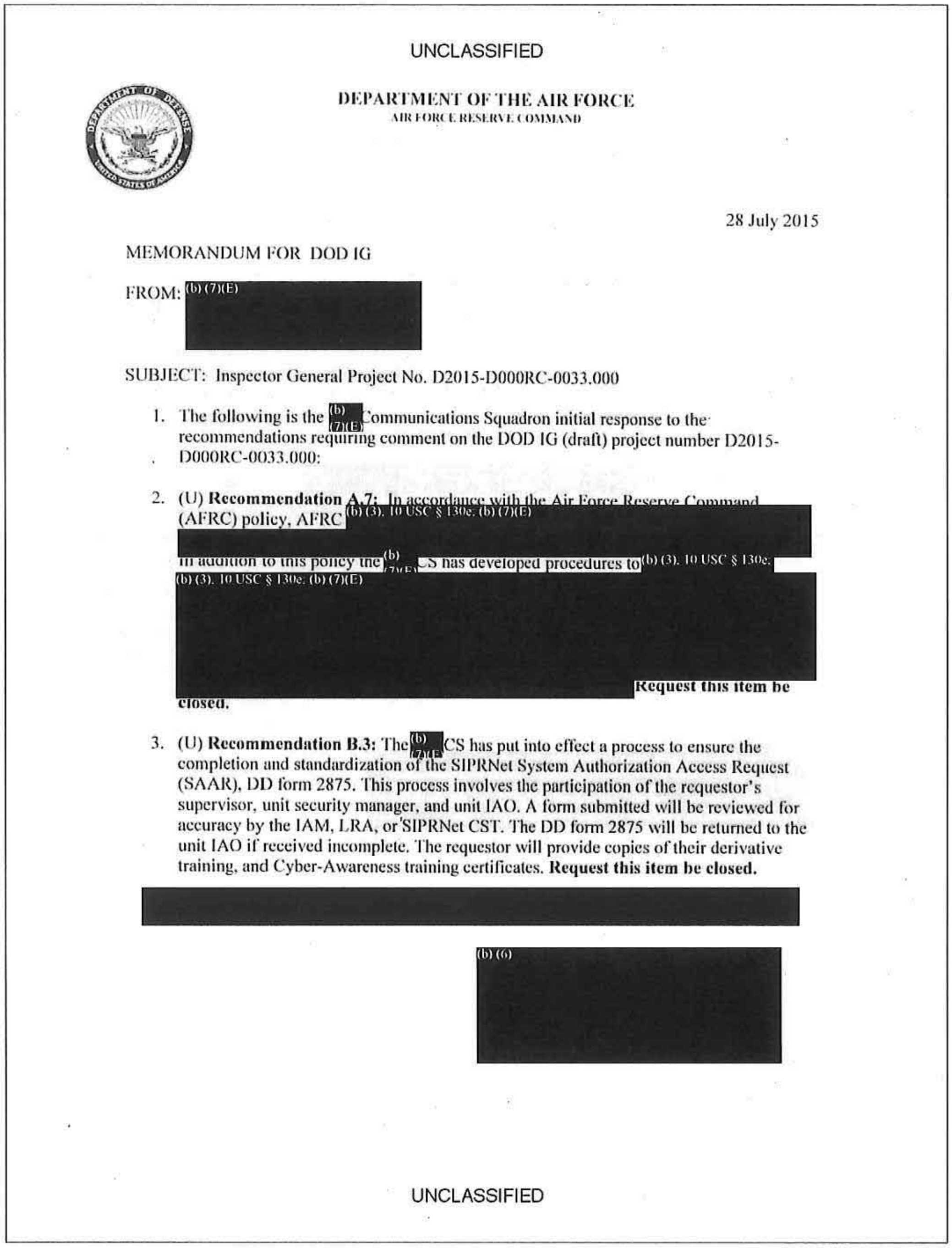
(b) (6) [redacted]

Attachments:
1. (b) (7)(E) [redacted]
2.
3.

CLASSIFICATION: **UNCLASSIFIED**

2

(U) (b)(7)(E) [redacted] Communications Squadron



UNCLASSIFIED

DEPARTMENT OF THE AIR FORCE
AIR FORCE RESERVE COMMAND

28 July 2015

MEMORANDUM FOR DOD IG

FROM: (b)(7)(E) [redacted]

SUBJECT: Inspector General Project No. D2015-D000RC-0033.000

1. The following is the (b)(7)(E) [redacted] Communications Squadron initial response to the recommendations requiring comment on the DOD IG (draft) project number D2015-D000RC-0033.000:

2. (U) **Recommendation A.7:** In accordance with the Air Force Reserve Command (AFRC) policy, AFRC (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] In addition to this policy the (b)(7)(E) [redacted] CS has developed procedures to (b)(3), 10 USC § 130e, [redacted] (b)(3), 10 USC § 130e, (b)(7)(E) [redacted] **Request this item be closed.**

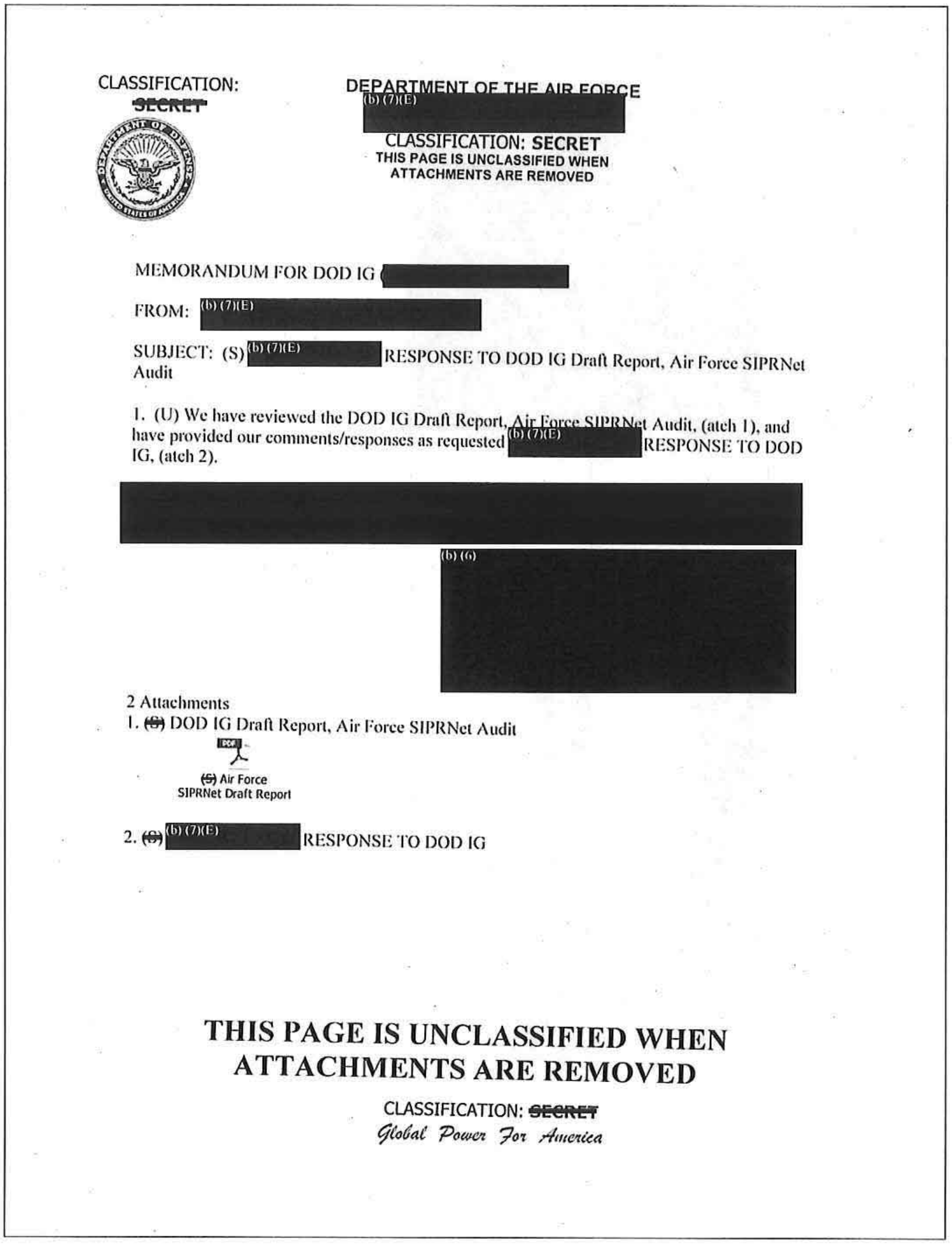
3. (U) **Recommendation B.3:** The (b)(7)(E) [redacted] CS has put into effect a process to ensure the completion and standardization of the SIPRNet System Authorization Access Request (SAAR), DD form 2875. This process involves the participation of the requestor's supervisor, unit security manager, and unit IAO. A form submitted will be reviewed for accuracy by the IAM, LRA, or SIPRNet CST. The DD form 2875 will be returned to the unit IAO if received incomplete. The requestor will provide copies of their derivative training, and Cyber-Awareness training certificates. **Request this item be closed.**

[redacted]

(b)(6) [redacted]

UNCLASSIFIED

(U) (b) (7)(E) Communications Squadron



CLASSIFICATION:
~~SECRET~~

DEPARTMENT OF THE AIR FORCE
(b) (7)(E)

CLASSIFICATION: SECRET
THIS PAGE IS UNCLASSIFIED WHEN
ATTACHMENTS ARE REMOVED

MEMORANDUM FOR DOD IG ([redacted]

FROM: (b) (7)(E)

SUBJECT: (S) (b) (7)(E) RESPONSE TO DOD IG Draft Report, Air Force SIPRNet Audit

1. (U) We have reviewed the DOD IG Draft Report, Air Force SIPRNet Audit, (atch 1), and have provided our comments/responses as requested (b) (7)(E) RESPONSE TO DOD IG, (atch 2).

[redacted]

(b) (6)

2 Attachments
1. ~~(S)~~ DOD IG Draft Report, Air Force SIPRNet Audit

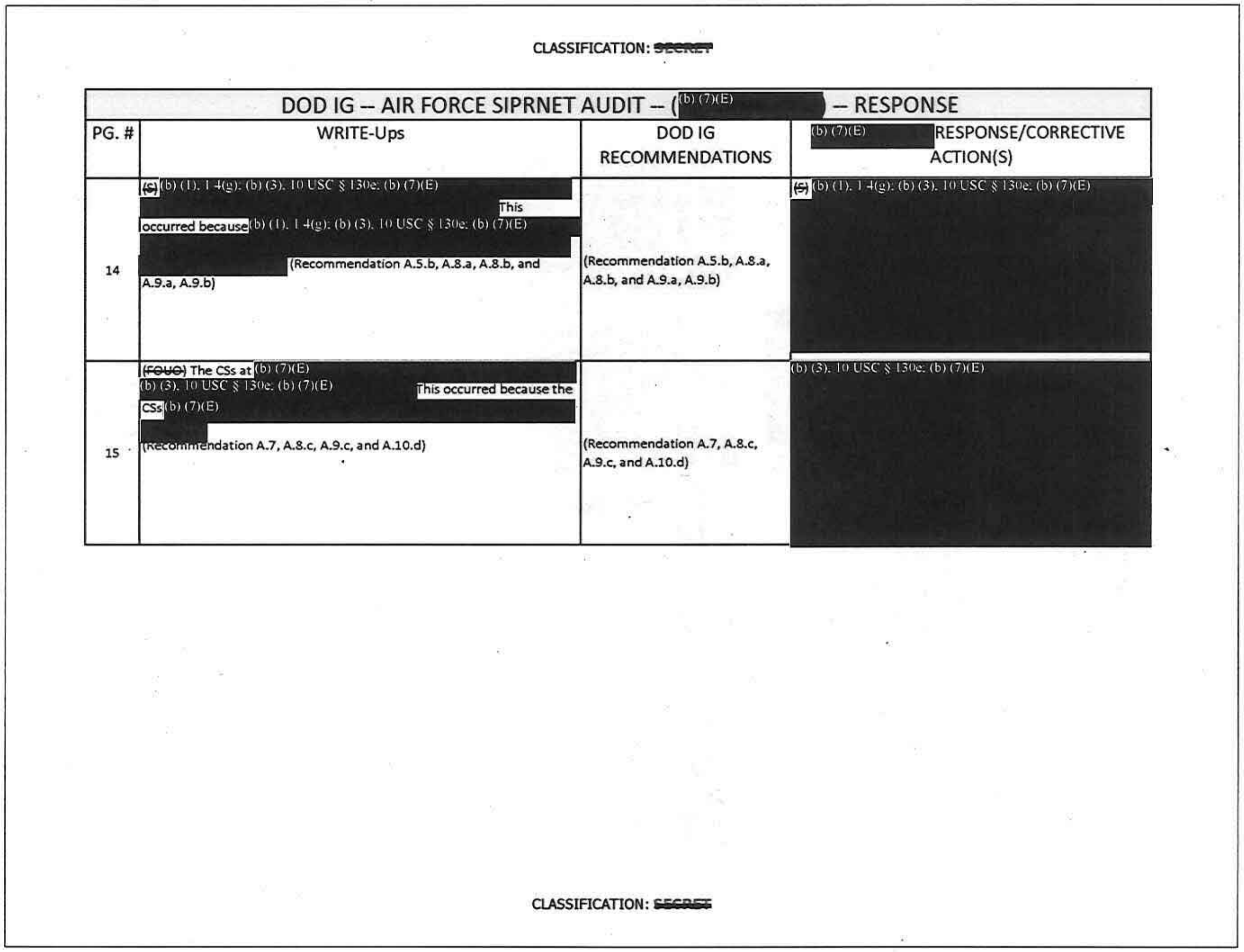
~~(S)~~ Air Force
SIPRNet Draft Report

2. ~~(S)~~ (b) (7)(E) RESPONSE TO DOD IG

THIS PAGE IS UNCLASSIFIED WHEN ATTACHMENTS ARE REMOVED

CLASSIFICATION: ~~SECRET~~
Global Power For America

(U) (b) (7)(E) [redacted] Communications Squadron (cont'd)

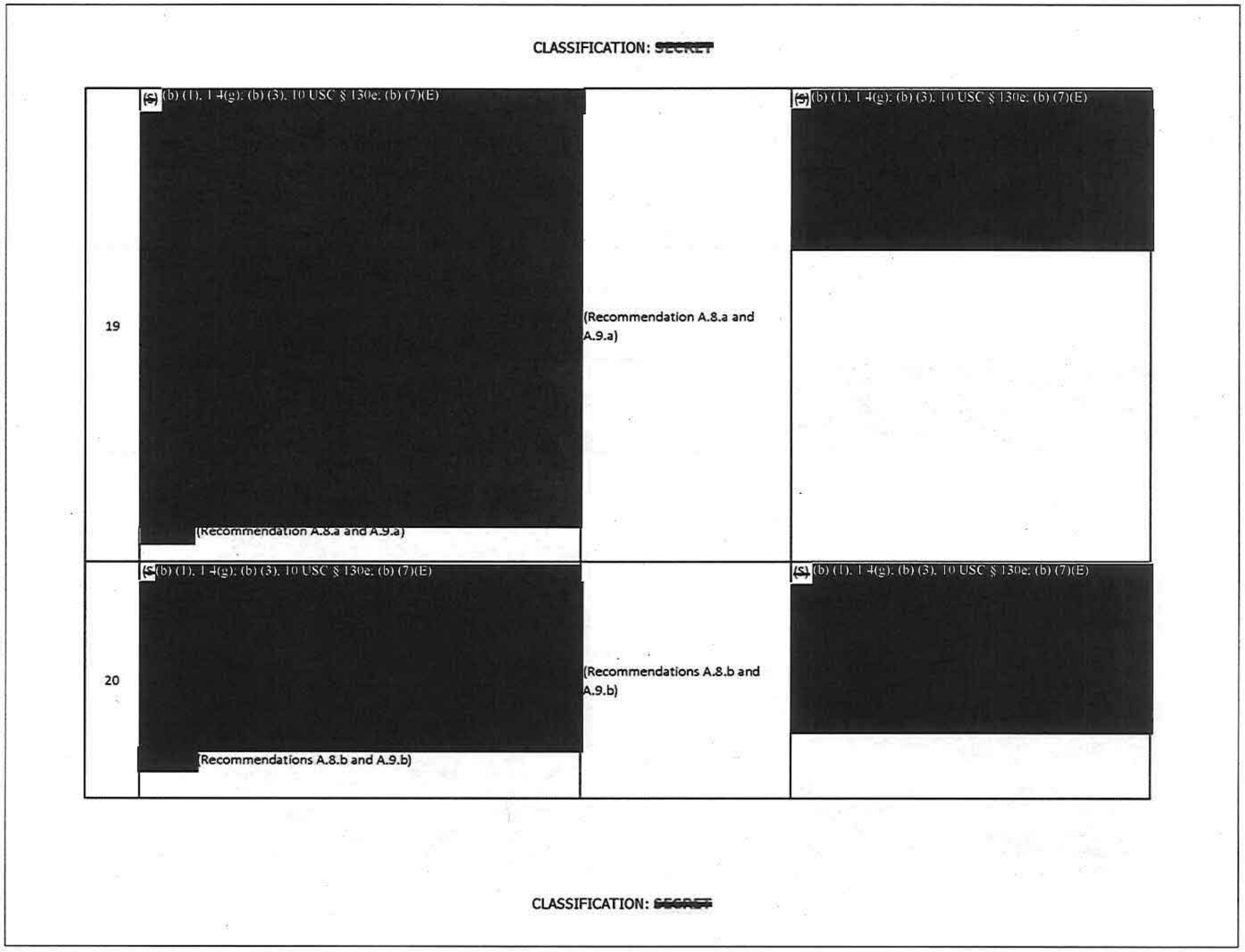


CLASSIFICATION: ~~SECRET~~

DOD IG -- AIR FORCE SIPRNET AUDIT -- ((b) (7)(E) [redacted]) -- RESPONSE			
PG. #	WRITE-Ups	DOD IG RECOMMENDATIONS	(b) (7)(E) [redacted] RESPONSE/CORRECTIVE ACTION(S)
14	~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] This occurred because (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] (Recommendation A.5.b, A.8.a, A.8.b, and A.9.a, A.9.b)	(Recommendation A.5.b, A.8.a, A.8.b, and A.9.a, A.9.b)	~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
15	~~(FOUO)~~ The CSs at (b) (7)(E) [redacted] (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] This occurred because the CSs (b) (7)(E) [redacted] (Recommendation A.7, A.8.c, A.9.c, and A.10.d)	(Recommendation A.7, A.8.c, A.9.c, and A.10.d)	(b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

CLASSIFICATION: ~~SECRET~~

(U) (b) (7)(E) [redacted] Communications Squadron (cont'd)



CLASSIFICATION: ~~SECRET~~

19	~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] [redacted] (Recommendation A.8.a and A.9.a)	(Recommendation A.8.a and A.9.a)	~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
20	~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] [redacted] (Recommendations A.8.b and A.9.b)	(Recommendations A.8.b and A.9.b)	~~(S)~~ (b) (1), 1.4(g); (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]

CLASSIFICATION: ~~SECRET~~

(U) (b) (7)(E) [redacted] Communications Squadron (cont'd)

CLASSIFICATION: ~~SECRET~~

24	~~(FOUO)~~ This occurred because (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]. The Commander, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] according to DoD and Air Force guidance. If (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] cannot be developed then the Commander, (b) (7)(E) [redacted] should coordinate with base CSs and any other necessary parties to develop a (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] he Commander, (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] in accordance with DoD and Air Force guidance. (Recommendations A.7.b, A.8.c, A.9.c, and A.10.d)	(Recommendations A.7.b, A.8.c, A.9.c, and A.10.d)	(U) Processes are now in place (b) (3), 10 USC § 130e; (b) (7) [redacted] It will be the members responsibility to contact their ISSO and/or CSA to (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
29	~~(FOUO)~~ (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] n accordance with applicable DoD and Air Force guidance.41 This occurred because [redacted] (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] (Recommendation B.4.a, B.4.b, B.4.c)	(Recommendation B.4.a, B.4.b, B.4.c)	(U) (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
29	~~(FOUO)~~ (b) (7)(E) [redacted] did not properly approve SIPRNet user access forms. This occurred because the CSs did not have effective policies and procedures to approve SIPRNet access. (Recommendation B.3, B.4.d, and B.5)	(Recommendation B.3, B.4.d, and B.5)	(U) Processes are currently in place to ensure that all documents (DD2875, DD2842, SF412, IA Training, and user agreements) are properly filled out prior to submitting a SIPR account request by the unit ISSO. This has been briefed to SQ, group, & wing commanders.

CLASSIFICATION: ~~SECRET~~

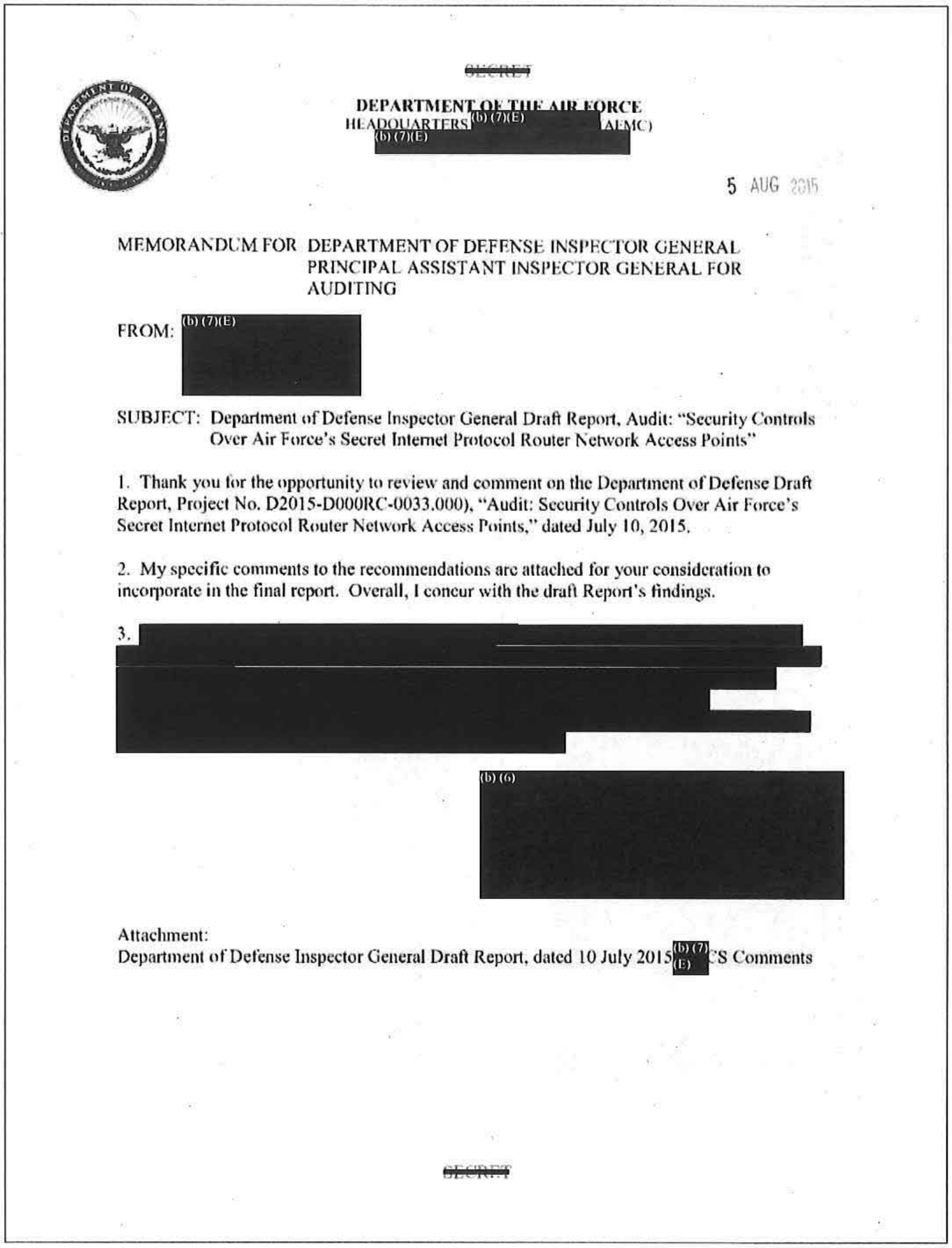
(U) (b) (7)(E) [redacted] Communications Squadron (cont'd)

CLASSIFICATION: ~~SECRET~~

31	~~(FOUO)~~ This occurred because (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] The Commander (b) (7)(E) [redacted] should develop and implement a plan to (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] In addition, the Commander, (b) (7)(E) [redacted] should immediately (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] (Recommendation B.4.a, B.4.b, and B.4.c)	(Recommendation B.3, B.4.d, and B.5)	(U) (b) (3), 10 USC § 130e; (b) (7)(E) [redacted]
34	~~(FOUO)~~ This occurred because the CSs did not establish policies and procedures to verify that all IAOs completed and approved forms required for network access before they provided users with SIPRNet access. (b) (3), 10 USC § 130e; (b) (7)(E) [redacted] The Commander, (b) (7)(E) [redacted] should develop procedures to verify that access forms are accurately completed before access to the SIPRNet is granted. (Recommendation B.3, B.4.d, and B.5)	(Recommendation B.3, B.4.d, and B.5)	(U) Processes are currently in place to ensure that all documents (DD2875, DD2842, SF412, IA Training, and user agreements) are properly filled out prior to submitting a SIPR account request by the unit ISSO. This has been briefed to SQ, group, & wing commanders.

CLASSIFICATION: ~~SECRET~~

(U) (b)(7)(E) [redacted] Mission Support Group



~~SECRET~~

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS (b)(7)(E) [redacted] AFMC)
(b)(7)(E) [redacted]

5 AUG 2015

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL
PRINCIPAL ASSISTANT INSPECTOR GENERAL FOR AUDITING

FROM: (b)(7)(E) [redacted]

SUBJECT: Department of Defense Inspector General Draft Report, Audit: "Security Controls Over Air Force's Secret Internet Protocol Router Network Access Points"

1. Thank you for the opportunity to review and comment on the Department of Defense Draft Report, Project No. D2015-D000RC-0033.000), "Audit: Security Controls Over Air Force's Secret Internet Protocol Router Network Access Points," dated July 10, 2015.

2. My specific comments to the recommendations are attached for your consideration to incorporate in the final report. Overall, I concur with the draft Report's findings.

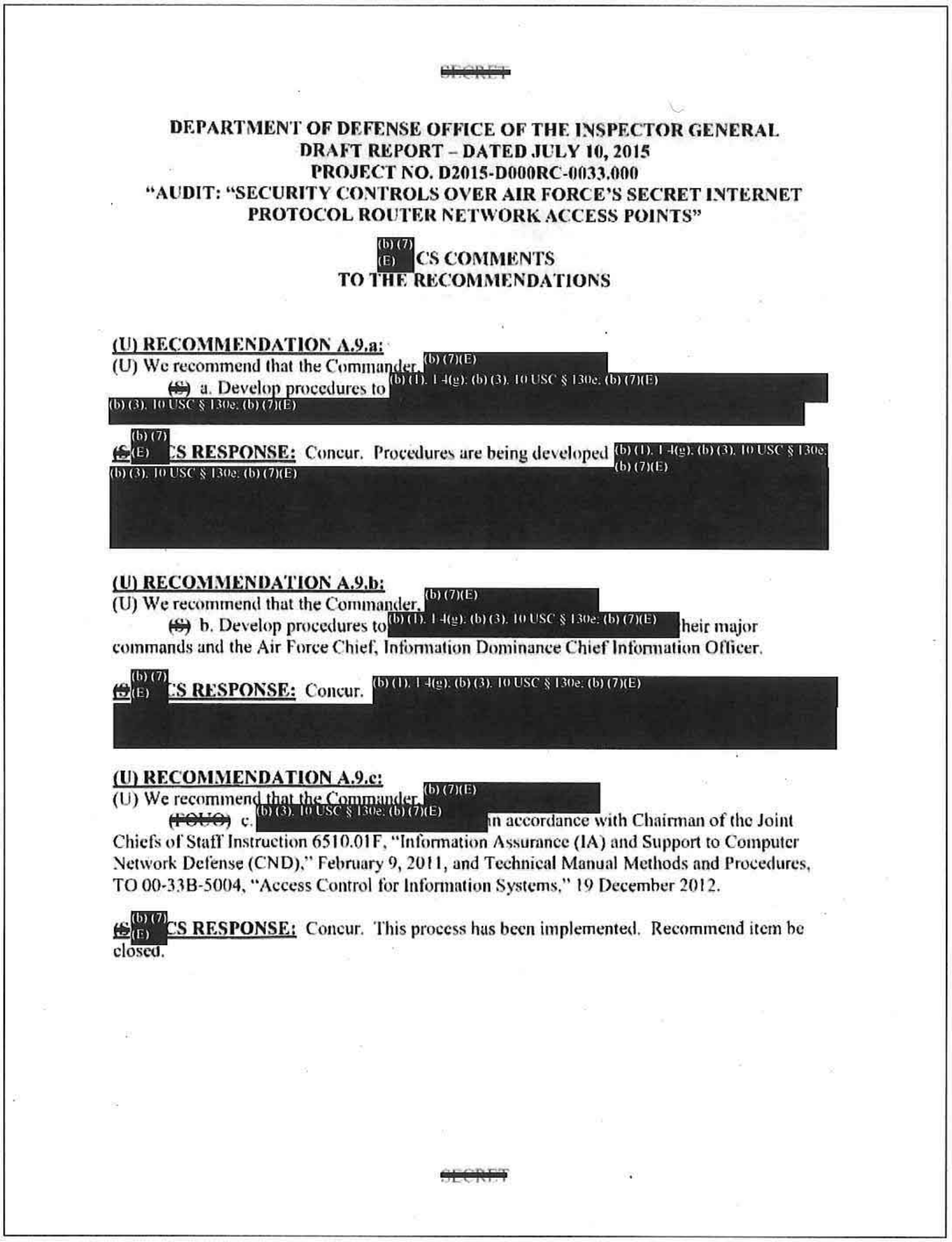
3. [redacted]

(b)(6) [redacted]

Attachment:
Department of Defense Inspector General Draft Report, dated 10 July 2015 (b)(7)(E) [redacted] CS Comments

~~SECRET~~

(U) (b)(7)(E) [redacted] Mission Support Group (cont'd)



~~SECRET~~

DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL
DRAFT REPORT – DATED JULY 10, 2015
PROJECT NO. D2015-D000RC-0033.000
"AUDIT: "SECURITY CONTROLS OVER AIR FORCE'S SECRET INTERNET PROTOCOL ROUTER NETWORK ACCESS POINTS"

(b)(7)(E) [redacted] CS COMMENTS
TO THE RECOMMENDATIONS

(U) RECOMMENDATION A.9.a:
(U) We recommend that the Commander, (b)(7)(E) [redacted]

~~(S)~~ a. Develop procedures to (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) (b)(3), 10 USC § 130e; (b)(7)(E) [redacted]

~~(S~~ (b)(7)(E) [redacted] **CS RESPONSE:** Concur. Procedures are being developed (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) (b)(3), 10 USC § 130e; (b)(7)(E) [redacted]

(U) RECOMMENDATION A.9.b:
(U) We recommend that the Commander, (b)(7)(E) [redacted]

~~(S)~~ b. Develop procedures to (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) [redacted] heir major commands and the Air Force Chief, Information Dominance Chief Information Officer.

~~(S)~~ (b)(7)(E) [redacted] **CS RESPONSE:** Concur. (b)(1), 1.4(g); (b)(3), 10 USC § 130e; (b)(7)(E) [redacted]

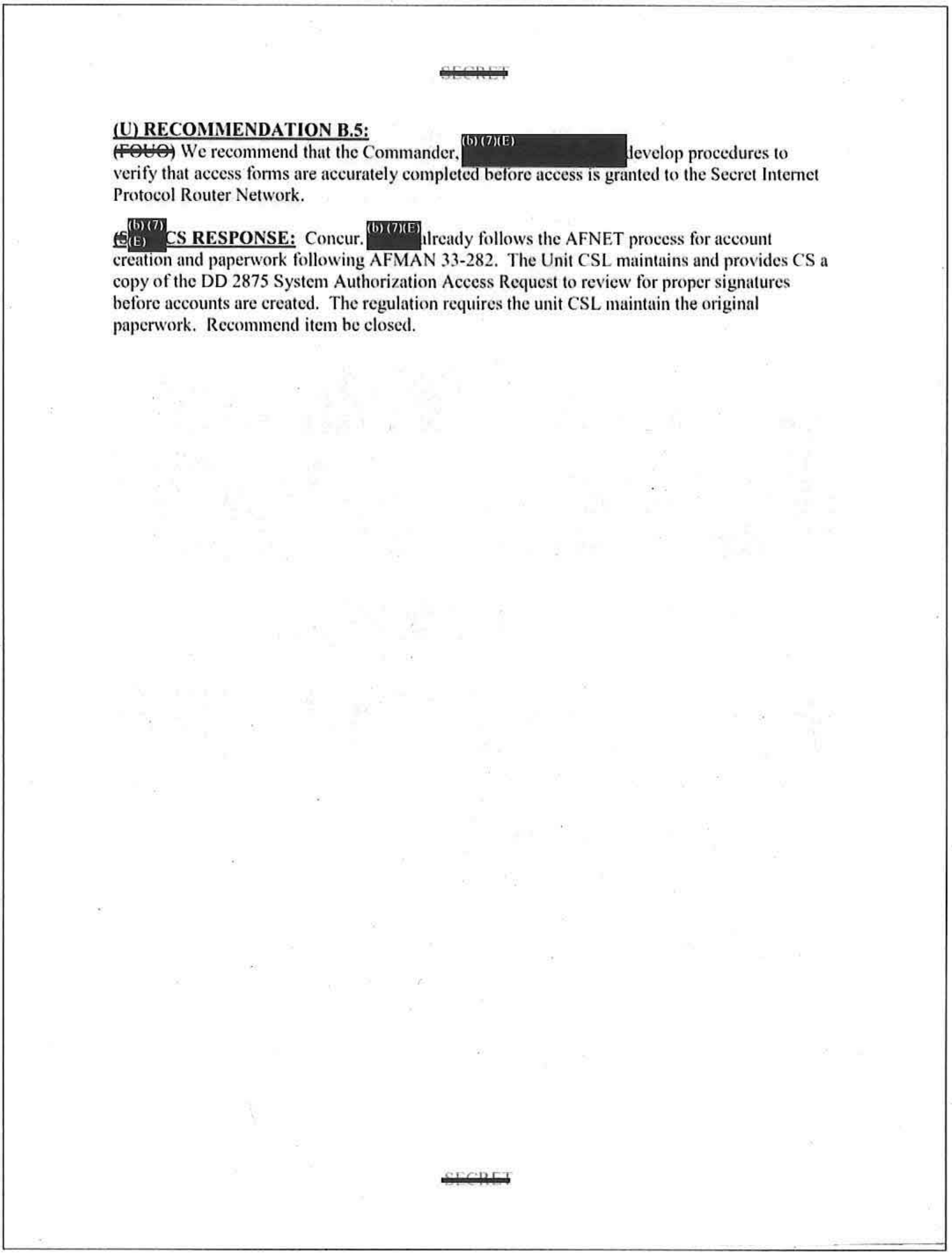
(U) RECOMMENDATION A.9.c:
(U) We recommend that the Commander, (b)(7)(E) [redacted]

~~(FOUO)~~ c. (b)(3), 10 USC § 130e; (b)(7)(E) [redacted] n accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, and Technical Manual Methods and Procedures, TO 00-33B-5004, "Access Control for Information Systems," 19 December 2012.

~~(S)~~ (b)(7)(E) [redacted] **CS RESPONSE:** Concur. This process has been implemented. Recommend item be closed.

~~SECRET~~

(U) (b) (7)(E) Mission Support Group (cont'd)



~~SECRET~~

(U) RECOMMENDATION B.5:
~~(FOUO)~~ We recommend that the Commander, (b) (7)(E) develop procedures to verify that access forms are accurately completed before access is granted to the Secret Internet Protocol Router Network.

~~(S~~(b) (7)(E) **CS RESPONSE:** Concur. (b) (7)(E)lready follows the AFNET process for account creation and paperwork following AFMAN 33-282. The Unit CSL maintains and provides CS a copy of the DD 2875 System Authorization Access Request to review for proper signatures before accounts are created. The regulation requires the unit CSL maintain the original paperwork. Recommend item be closed.

~~SECRET~~

(U) Acronyms and Abbreviations

AFB	Air Force Base
ARB	Air Reserve Base
ATO	Authorization to Operate
CAT	Category
CIO	Chief Information Officer
(b)(7)(E)	
CS	Communications Squadron
DIACAP	DoD Information Assurance Certification and Accreditation Process
HBSS	Host Based Security System
IA	Information Assurance
IAO	Information Assurance Officer
IP	Internet Protocol
IT	Information Technology
NATO	North Atlantic Treaty Organization
NOS	Network Operations Squadron
PDS	Protected Distribution System
POA&M	Plan of Actions and Milestones
RSD	Rogue System Detection
SAF/CIO A6	Air Force Chief Information Officer
SIPRNet	Secret Internet Protocol Router Network

(U) Glossary

(U) **Active Directory.** Provides a method to store data and provide the data to network users and administrators.

(U) **Allow-all.** A configuration that allows all traffic to flow through without security evaluation.

(U) **Authorization to Operate (ATO).** Authorization granted by a designated accrediting authority for a DoD information system to process, store, or transmit information; an ATO indicates a DoD information system has adequately implemented all assigned information assurance controls to the point where residual risk is acceptable to the designated accrediting authority. ATOs may be issued for up to 3 years.

(U) **Boundary Protection.** Monitoring and controlling communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices.

(U) **Deny-by-default.** A configuration in which network traffic, which is not expressly allowed, is denied.

(U) **Disable.** To configure the enclave firewalls to be routers and allow-all network traffic.

(U) **DoD Components.** Combatant commands, Military Services, Federal agencies, and field activities.

(U) **Enclave.** A collection of information systems connected by one or more internal networks under the control of a single authority and security policy.

(U) **Enclave Perimeter.** Includes those points where remote users of an enclave gain access to resources and information within that enclave, or where members of the enclave, but not physically located within the enclave, gain access to resources or information within that enclave.

(U) **Firewalls.** Hardware and software that limits access between networks or systems (or both) in accordance with a specific security policy.

(U) **Gateways.** Entry and exit points for data to and from the SIPRNet.

(U) **Host Based Security System (HBSS).** An application that monitors, detects, and counters against known cyber threats.

(U) **Logical Safeguards.** System-based mechanisms such as firewalls, permission settings, usernames and passwords, and SIPRNet tokens that are used to designate who or what has access to a specific system or function.

(U) **Interim Authorization to Operate.** Temporary authorization granted by the designated accrediting authority to operate a DoD information system under the conditions or constraints enumerated in the accreditation decision.

(U) **Internet Protocol (IP) Address.** Identifiers that are assigned to equipment connected to the network.

(U) **Network Defense Devices.** Network defense devices include equipment used to monitor, detect, analyze, and respond and restore activities.

(U) **Physical Safeguards.** Locks, guards, and security containers deter or delay an adversary's access to the network.

(U) **Plan of Action and Milestones (POA&M).** A permanent record that identifies tasks to be accomplished to resolve vulnerabilities; required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document designated accrediting authority accepted noncompliant information assurance controls and baseline information assurance controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

(U) **Port Security.** To electronically lock network ports so that only approved devices can use the port.

(U) **Protected Distribution System (PDS).** A system used to transmit encrypted classified National Security Information through an area of lesser classification or control.

(U) **Removable Media.** Items such as compact discs, digital video discs, secure digital cards, tape, flash memory data storage devices, diskettes, multi-media cards, and external hard drives.

(U) **Rouge System Device (RSD).** Device that does not have Host Based Security System software installed.

(U) **Security Posture.** The security status of an enterprise's networks, information, and systems based on information assurance resources and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

(U) **Severity Category (CAT) I.** Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumptions of super-user privileges. An ATO will not be granted while CAT I weaknesses are present.

(U) **Subnetwork.** An identifiably separate part of an organization's network.

(U) **Validation.** Confirmation that requirements for a specific intended use or application have been fulfilled.

(U) **Write Function.** The ability to download or transfer data from the SIPRNet to removable media.

(U) Annex

(U) Sources

(~~FOUO~~) Source 1: DoD Instruction O-3600.02, “Information Operations (IO) Security Classification Guide,” November 28, 2005 (Document For Official Use Only)

(~~FOUO~~) Source 2: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20241114

Date of Source: November 14, 2014

(~~FOUO~~) Source 3: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20241114

Date of Source: November 14, 2014

(~~FOUO~~) Source 4: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20241209

Date of Source: December 9, 2014

(~~FOUO~~) Source 5: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20241209

Date of Source: December 9, 2014

(~~FOUO~~) Source 6: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250114

Date of Source: January 14, 2015

(~~FOUO~~) Source 7: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250114

Date of Source: January 14, 2015

~~(FOUO)~~ Source 8: “(b)(7)(E) [redacted] CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250211

Date of Source: February 11, 2015

~~(FOUO)~~ Source 9: “(b)(7)(E) [redacted] Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250211

Date of Source: February 11, 2015

~~(FOUO)~~ Source 10: “(b)(7)(E) [redacted] CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250305

Date of Source: March 5, 2015

~~(FOUO)~~ Source 11: “(b)(7)(E) [redacted] Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250305

Date of Source: March 5, 2015

~~(FOUO)~~ Source 12: “(b)(7)(E) [redacted] CCRI Summary Report,” (Document classified Secret)

Declassify On: 20241201

Date of Source: December 1, 2014

~~(FOUO)~~ Source 13: “(b)(7)(E) [redacted] Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20241201

Date of Source: December 1, 2014

~~(FOUO)~~ Source 14: “(b)(7)(E) [redacted] CCRI Summary Report,” (Document classified Secret)

Declassify On: 20241204

Date of Source: December 4, 2014

~~(FOUO)~~ Source 15: “(b)(7)(E) [redacted] Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20241204

Date of Source: December 4, 2014

~~(FOUO)~~ Source 16: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250108

Date of Source: January 8, 2015

~~(FOUO)~~ Source 17: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250108

Date of Source: January 8, 2015

~~(FOUO)~~ Source 18: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250205

Date of Source: February 5, 2015

~~(FOUO)~~ Source 19: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250205

Date of Source: February 5, 2015

~~(FOUO)~~ Source 20: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250305

Date of Source: March 5, 2015

~~(FOUO)~~ Source 21: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250305

Date of Source: March 5, 2015

~~(FOUO)~~ Source 22: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20241117

Date of Source: November 17, 2014

~~(FOUO)~~ Source 23: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20241117

Date of Source: November 17, 2014

~~(FOUO)~~ Source 24: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20241203

Date of Source: December 3, 2014

~~(FOUO)~~ Source 25: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20241203

Date of Source: December 3, 2014

~~(FOUO)~~ Source 26: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250108

Date of Source: January 8, 2015

~~(FOUO)~~ Source 27: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250108

Date of Source: January 8, 2015

~~(FOUO)~~ Source 28: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250205

Date of Source: February 5, 2015

~~(FOUO)~~ Source 29: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250205

Date of Source: February 5, 2015

~~(FOUO)~~ Source 30: “(b)(7)(E) CCRI Summary Report,” (Document classified Secret)

Declassify On: 20250313

Date of Source: March 13, 2015

~~(FOUO)~~ Source 31: “(b)(7)(E) Technical Vulnerability Report,” (Document classified Secret)

Declassify On: 20250313

Date of Source: March 13, 2015

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

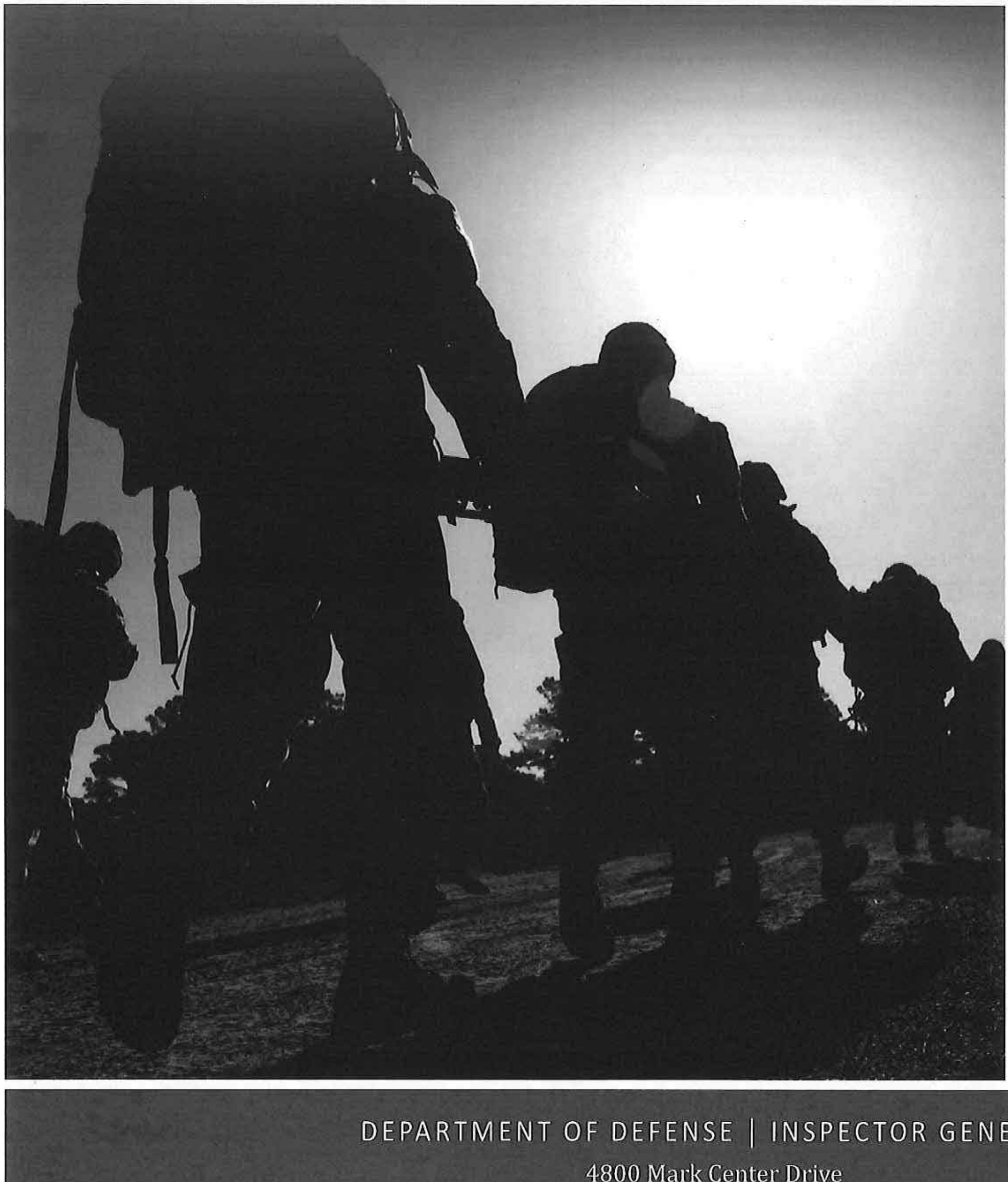
Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098